TRƯỜNG ĐẠI HỌC ĐÀ LẠT

GIÁO TRÌNH

ĐẠI SỐ ĐẠI CƯƠNG

ĐỖ NGUYÊN SƠN

2000

MỤC LỤC

CHƯƠNG 1:
ĐẠI CƯƠNG VỀ CẤU TRÚC ĐẠI SỐ

1. Tập hợp - Ánh xạ - Quan hệ.

1.1 Tập hợp.

• **Tập hợp** là một khái niệm ban đầu. Tập hợp được mô tả như một tòan thể nào đó bao gồm những đối tượng nào đó có cùng một dấu hiệu hay một tính chất nhất định. Các đối tượng lập nên tập hợp gọi là **phần tử**. Ta thường kí hiệu các tập hợp bằng các chữ cái A, B, X, Y.... còn các phần tử của chúng bằng các chữ cái nhỏ a, b, x, y… Có hai cách để xác định một tập hợp, một là liệt kê ra tất cả các phần tử của nó, $A = \{a_1, a_2, \ldots a_n\}$; hai là miêu tả đặc tính các phần tử tạo nên tập hợp, $X = \{x : x \text{ có tính chất } E\}$. Nếu a là phần tử của tập hợp A thì ta viết $a \in A$. Nếu a không là phần tử của tập hợp A thì ta viết $a \notin A$. Tập hợp không chứa một phần tử nào được gọi là **tập hợp rỗng** và kí hiệu là $\varnothing$.

Ví dụ, các tập hợp số mà ta đã quen biết : **tập các số tự nhiên (không có số 0)** $\angle = \{1, 2, 3, \ldots, n, \ldots\}$; tập số tự nhiên (với số 0), $\angle_0 = \{0, 1, 2, \ldots, n, \ldots\}$; **tập các số nguyên** $9 = \{0, \pm 1, \pm 2, \ldots, \pm n, \ldots\}$; **tập các số hữu tỉ** $\Theta = \{\frac{m}{n} : m \in 9, n \in \angle\}$; **tập các số thực** 3; **tập các số phức** $\forall = \{a + bi : a, b \in 3\}$.

• Nếu mọi phần tử của tập hợp A đều là các phần tử của tập hợp B thì ta nói A nằm trong B, hay B chứa A, hay A là **tập con** của B , và kí hiệu là $A \subset B$ hoặc $B \supset A$.

• **Hợp của hai tập hợp** A và B là một tập hợp gồm tất cả các phần tử thuộc ít nhất một trong các tập hợp đã cho. Hợp của hai tập hợp được kí hiệu là $A \cup B$. **Hợp của họ các tập hợp** $\{A_\alpha\}$ là một tập hợp B gồm tất cả các phần tử thuộc ít nhất một trong các tập hợp A_α và được kí hiệu là $B = \bigcup_\alpha A_\alpha$

• VÍ DỤ: $\bigcup_{n=1}^{\infty} [0, 1 - \frac{1}{n}] = [0, 1)$

• **Giao của hai tập hợp** A và B là một tập hợp gồm tất cả các phần tử đồng thời thuộc tập hợp A và tập hợp B. Giao của hai tập hợp được kí hiệu là $A \cap B$.

• **Giao của họ các tập hợp** $\{A_\alpha\}$ là một tập hợp B gồm tất cả các phần tử đồng thời thuộc vào mọi tập hợp A_α và được kí hiệu là $B = \bigcap_\alpha A_\alpha$.

• VÍ DỤ: $\bigcap_{n=1}^{\infty} [-\frac{1}{n}, \frac{1}{n}] = \{0\}$

• Hợp và giao các tập hợp có các tính chất

1) $A \cup B = B \cup A$ $\qquad A \cap B = B \cap A$ (Giao hóan)
2) $A \cup (B \cup C) = (A \cup B) \cup C$ $\qquad A \cap (B \cap C) = (A \cap B) \cap C$ (Kết hợp)

3) $A\cap(\bigcup_{\alpha} A_\alpha) = \bigcup_{\alpha}(A\cap A_\alpha)$ $\qquad A\cup(\bigcap_{\alpha} A_\alpha) = \bigcap_{\alpha}(A\cup A_\alpha)$ (Phân phối)

• **Hiệu của hai tập hợp** A và B là một tập hợp gồm tất cả các phần tử của tập hợp A mà không phải là phần tử của tập hợp B. Hiệu của hai tập hợp được kí hiệu là $A \setminus B$ hay $A - B$

• **Hiệu đối xứng của hai tập hợp** A và B là tập hợp $(A - B)\cup(B - A)$. Hiệu đối xứng của hai tập hợp được kí hiệu là $A\Delta B$. Rõ ràng rằng $A\Delta B = B\Delta A$.

• **Tích trực tiếp** hay **tích Descartes** của hai tập hợp A và B là một tập hợp gồm mọi cặp (x,y) ở đây $x\in A$ và $y\in B$, và được kí hiệu là $A\times B$.
Tích Descartes của họ các tập hợp $\{A_\alpha\}_{\alpha\in I}$ là một tập hợp gồm các họ $(a_\alpha)_{\alpha\in I}$, với $a_\alpha\in A_\alpha$ với mọi $\alpha\in I$, và được kí hiệu là $\prod_{\alpha\in I} A_\alpha$.

• Nếu B là tập con của tập hợp A thì $A - B$ được gọi là phần bù của tập hợp B đối với tập hợp A và được kí hiệu là $\mathbf{C}_A B$. Đối với phần bù ta có luật đối ngẫu

$$\mathbf{C}(\bigcup_{\alpha} A_\alpha) = \bigcap_{\alpha}(\mathbf{C}A_\alpha) \quad \mathbf{C}(\bigcap_{\alpha} A_\alpha) = \bigcup_{\alpha}(\mathbf{C}A_\alpha).$$

1.2 Ánh xạ

• Cho hai tập hợp X và Y. Một **ánh xạ** từ X vào Y là một qui luật f nào đó cho tương ứng một phần tử $x\in X$ với duy nhất một phần tử $y\in Y$. X được gọi là tập nguồn hay miền xác định còn Y là tập đích hay miền giá trị. Phần tử y được gọi là **ảnh** của x, còn x được gọi là **tạo ảnh** của y qua ánh xạ f, khi đó ta viết $y = f(x)$. Để chỉ một ánh xa từ X vào Y thường dùng kí hiệu

$$f : X \to Y,\ x \mapsto y = f(x)$$

• Cho ánh xạ $f : X \to Y$ và U, V lần lượt là các tập con của X và Y. Tập hợp $f(U) = \{f(x) : x\in U\}$ được gọi là **ảnh của tập hợp U qua ánh xạ f**, còn tập hợp $f^{-1}(V) = \{x\in X : f(x)\in V\}$ được gọi là **nghịch ảnh của tập hợp V**.

• Ánh xạ $f|_U : U\to Y$, xác định bởi $f|_U(x) = f(x)$ với mọi $x\in U$, được gọi là **hạn chế của ánh xạ f trên U**. Ánh xạ $id_X : X \to X$, $id_X(x) = x$, được gọi là **ánh xạ đồng nhất trên X**.

• Ta có các tính chất sau

$$A, B\subset X \Rightarrow \begin{cases} f(A\cup B) = f(A)\cup f(B) \\ f(A\cap B)\subset f(A)\cap f(B) \end{cases}$$

$$U, V \subset Y \Rightarrow \begin{cases} f^{-1}(U \cup V) = f^{-1}(U) \cup f^{-1}(V) \\ f^{-1}(U \cap V) = f^{-1}(U) \cap f^{-1}(V) \end{cases}$$

CHÚ Ý : Đẳng thức $f(A \cap B) = f(A) \cap f(B)$ nói chung không đúng. Chẳng hạn, xét ánh xạ $f : 3 \to 3$, $f(x) = \sin x$; và $A = [0, \frac{3\pi}{4}]$, $B = [\frac{\pi}{2}, \frac{3\pi}{2}]$.

• Hai ánh xạ $f_1 : X_1 \to Y_1$ và $f_2 : X_2 \to Y_2$ được gọi là **bằng nhau** nếu $X_1 = X_2$ và $f_1(x) = f_2(x)$ với mọi $x \in X_1$, khi đó ta viết $f_1 = f_2$.

• Cho hai ánh xạ $f : X \to Y$ và $g : Y \to Z$. **Hợp của f với g**, ký hiệu là gof, là ánh xạ từ X vào Z, được xác định bởi $(gof)(x) = g(f(x))$. Nếu $h : Z \to T$ là một ánh xạ khác thì ta có $ho(gof) = (hog)o f$.

• Ánh xạ $f : X \to Y$ được gọi là **đơn ánh** nếu ảnh của hai phần tử khác nhau trong X là hai phần tử khác nhau trong Y. Ánh xạ f được gọi là **tòan ánh** nếu $f(X) = Y$, tức là đối với mỗi phần tử $y \in Y$ tồn tại một phần tử $x \in X$ sao cho $y = f(x)$. Một ánh xạ vừa đơn ánh vừa tòan ánh được gọi là **song ánh.**

• Nếu $f : X \to Y$ là một song ánh thì đối với mỗi y thuộc Y có duy nhất một x thuộc X sao cho $y = f(x)$. Điều này cho phép xác định một ánh xạ f^{-1} từ Y vào X với $f^{-1}(y) := x$ nếu $f(x) = y$. Ánh xạ f^{-1} được gọi là **ánh xạ ngược của ánh xạ f**. Hiển nhiên rằng $f^{-1}o f = id_X$ và $f o f^{-1} = id_Y$. Ta cũng có thể dễ kiểm tra rằng, nếu $f : X \to Y$, $g : Y \to Z$ là các song ánh thì $f^{-1} : Y \to X$, $(g o f) : X \to Z$ cũng là các song ánh và $(g o f)^{-1} = f^{-1} o g^{-1}$.

1.3 Tập hữu hạn - vô hạn - đếm được

Nếu có một song ánh $f : X \to Y$ từ tập hợp X vào tập hợp Y thì ta nói X và Y **có cùng lực lượng**. Tập hợp X gọi là **đếm được** nếu nó cùng lực lượng với tập hợp các số tự nhiên $\angle$. Nói cách khác, tập hợp đếm được là tập hợp mà các phần tử của nó có thể đánh số thành dãy vô hạn $x_1, x_2, \ldots, x_n, \ldots$. Một tập hợp X gọi là **hữu hạn** nếu nó cùng lực lượng với tập hợp $\{n \in \angle : 1 \le n \le k_o\}$ (với k_o là một số tự nhiên nào đó). Tập hợp không hữu hạn gọi là **vô hạn.**

• VÍ DỤ:Tập hợp các số nguyên có cùng lực lượng với tập số tự nhiên vì ta có song ánh $f : 9 \to \angle$, được xác định bởi $f(n) = 2n + 1$ nếu $n \ge 0$, và $f(n) = 2|n|$ nếu $n < 0$.

1.4 Quan hệ hai ngôi.

• Quan hệ (hai ngôi) trên tập X là một tập con R của $X \times X$. Nếu cặp phần tử $(x, y) \in R$ thì ta nói x có quan hệ R vơi y, và viết x R y.

• Một quan hệ R trên tập X được gọi là có tính chất

1) **phản xạ** nếu $x R x, \forall x \in X$
2) **đối xứng** nếu $x R y \Rightarrow y R x$.
3) **phản xứng** nếu $x R y$ và $y R x \Rightarrow x = y$.
4) **bắc cầu** nếu $x R y$ và $y R z \Rightarrow x R z$.

• VÍ DỤ:
a) Quan hệ bé hơn " $\leq$ " thông thường trên tập $\angle$ là phản xạ, không đối xứng, phản xứng, bắc cầu.

b) Quan hệ vuông góc trong tập hợp các đường thẳng của mặt phẳng là đối xứng, không phản xạ, không phản xứng, không bắc cầu.

1.5 Quan hệ tương đương.

• Quan hệ R trên tập X được gọi là quan hệ tương đương nếu nó có các tính chất: **phản xạ**, **đối xứng** và **bắc cầu**. Người ta thường kí hiệu quan hệ tương đương R bằng dấu " ~ " và đọc " a ~ b" là a tương đương với b.

• Cho R là một quan hệ tương đương trên X. Đối với mỗi x thuộc X, tập hợp con $\{ y \in X : x R y \}$ của X được gọi là một **lớp tương đương của x** (modulo R) và được kí hiệu là $[x]_R$, hoặc [x], hoặc $\bar{x}$, hoặc $\hat{x}$. Mỗi phần tử của $[x]_R$ được gọi là một **đại diện** của $[x]_R$.

• Tập hợp $X/_R := \{ [x] : x \in X \}$ được gọi là **tập thương** của X đối với quan hệ tương đương R . Ánh xạ $\pi : X \to X/_R$, $\pi(x) = [x]$, là một tòan ánh và được gọi là **tòan cấu chính tắc.**

VÍ DỤ:
a) Quan hệ bằng nhau trong một tập hợp bất kì X là một quan hệ tương đương. Với mỗi x thuộc X, ta có [x] = {x} và $X/_R = \{\{x\}, x \in X\}$.

b) Với mỗi $n \in \angle$, quan hệ đồng dư modulo n trên 9, kí hiệu $x \equiv y(\text{mod } n)$ và đọc là " x là đồng dư với y modulo n ", được xác định bởi:

$$x \equiv y(\text{mod } n) \Leftrightarrow x - y \text{ chia hết cho } n$$

là một quan hệ tương đương. Lớp tương đương của x được gọi là lớp đồng dư modulo n của x , và thường được kí hiệu là $\bar{x} = \{x + kn, k \in 9 \}$.

• Một họ $P = \{X_\alpha\}_{\alpha \in I}$ cać tập con của X gọi là một **phân lớp** (hay **phân hoạch**) của X nếu

1) $X_\alpha \neq \varnothing$, $\forall \alpha \in I$.

2) $X = \bigcup_{\alpha \in I} X_\alpha$

3) $X_\alpha \cap X_\beta \neq \varnothing \Rightarrow X_\alpha = X_\beta$.

1.6 Mệnh đề

a) Nếu R là một quan hệ tương đương trong X thì tập thương $X/_R$ là một phân lớp của X.

b) Nếu $P = \{X_\alpha\}_{\alpha \in I}$ là một phân lớp của X thì $R(P) = \{(x,y) \in X \times X$: tồn tại $X_\alpha \in P$ để $x, y \in X_\alpha\}$ là một quan hệ tương đương trên X, và $P = X/_{R(P)}$.

Chứng minh:

a) Giả sử R là một quan hệ tương đương trong X.

• Vì nếu x thuộc X thì x thuộc [x] nên $[x] \neq \varnothing$ và $X = \bigcup_{x \in X} [x]$.

• Nếu $[x] \cap [y] \neq \varnothing$, tức là tồn tại $z \in [x] \cap [y]$. Khi đó zRx và zRy. Vì vậy xRy (do tính đối xứng và bắc cầu của R). Từ đó, [x]= [y].

b) Giả sử $P = \{X_\alpha\}_{\alpha \in I}$ là một phân lớp của X và R(P) là quan hệ trên X xác định bởi : $x\ R(P)\ y \Leftrightarrow \exists\ X_\alpha \in P, x, y \in X_\alpha$.

• Tính phản xạ và tính đối xứng của R(P) là rõ ràng. Giả sử $x, y, z \in X$ sao cho x R(P) y và y R(P) z. Khi đó tồn tại X_α và X_β sao cho $x, y \in X_\alpha$ và $y, z \in X_\beta$. Như vậy, $X_\alpha \cap X_\beta \neq \varnothing$ và do P là phân lớp của X nên $X_\alpha = X_\beta$. Từ đó, x, z thuộc $X_\alpha = X_\beta$, tức là x R(P) z. Điều này suy ra tính bắc cầu của R(P).

• Ta có nhận xét rằng, nếu $x \in X_\mathfrak{o}$ thì $[x]_{R(P)} = X_\mathfrak{o}$. Thật vậy, nếu lấy bất kì y thuộc $[x]_{R(P)}$ thì y R(P) x nên tồn tại $X_\beta \in P$ sao cho $y, x \in X_\beta$. Nhưng khi đó, vì X_β và $X_\mathfrak{o}$ có chung phần tử x nên trùng nhau; tức là y cũng là phần tử của $X_\mathfrak{o}$, điều này suy ra $[x]_{R(P)} \subset X_\mathfrak{o}$. Ngược lại, nếu lấy bất kì y thuộc $X_\mathfrak{o}$ thì do x cũng thuộc $X_\mathfrak{o}$ nên x R(P) y, tức là $y \in [x]_{R(P)}$. Từ đó, $X_\mathfrak{o} \subset [x]_{R(P)}$.

• Nhận xét trên suy ra phần còn lại của mệnh đề. □

• NHẬN XÉT :

a) Nếu R là một quan hệ tương đương trong X, thì với mọi x, y thuộc X ta có

$$x\ R\ y \Leftrightarrow [x] = [y] \Leftrightarrow x \in [y] \Leftrightarrow y \in [x]$$

b) Mệnh đề 1.6 cho thấy một sự tương ứng 1 – 1 giữa tập các quan hệ tương đương trên X và tập các phân hoạch của X.

1.7 Quan hệ thứ tự

• Quan hệ 2 ngôi R trên tập X được gọi là **quan hệ thứ tự không chặt** nếu nó có các tính chất **phản xạ**, **phản xứng** và **bắc cầu**, và được gọi là **quan hệ thứ tự chặt** nếu nó chỉ có các tính **phản xứng** và **bắc cầu** .

• Cho R là quan hệ thứ tự trên X. Hai phần tử a, b ∈ X được gọi là **so sánh được** đối với R nếu luôn luôn có a R b hoặc b R a. Một quan hệ thứ tự R trên X gọi là **quan hệ thứ tự tòan phần** nếu mọi cặp phần tử khác nhau của X đều so sánh được, còn trái lại thì được gọi là **quan hệ thứ tự bộ phận**.

• VÍ DỤ:

a) Quan hệ bé hơn ≤ thông thường trong 3 là một quan hệ thứ tự không chặt, tòan phần.

b) Quan hệ chia hết trong ∠, được kí hiệu là a ξ b và đọc là a chia hết b, là một quan hệ thứ tự không chặt, bộ phận.

c) Quan hệ bao hàm ⊂ trong tập các tập con của X là một quan hệ thứ tự bộ phận.

• Nếu R là một quan hệ thứ tự trong X thì ta thường kí hiệu R bằng dấu ≤ và đọc " a ≤ b " là " a bé hơn b". Ta xem kí hiệu b ≥ a là đồng nghĩa với a ≤ b và đọc là " b lớn hơn a ".

• Tập hợp X được gọi là **được sắp thứ tự** (hay **được sắp**) (chặt, không chặt, bộ phận, tòan phần) nếu trong nó có xác định một quan hệ thứ tự (chặt, không chặt, bộ phận, tòan phần) ≤ , và viết (X, ≤).

• Giả sử (X, ≤) là một tập được sắp. Phần tử a ∈ X gọi là **phần tử cực tiểu** (tương ứng: **cực đại**) của X khi và chỉ khi nếu có quan hệ x≤ a (tương ứng: x ≥a) thì kéo theo x = a . Phần tử a ∈ X gọi là **phần tử bé nhất** (tương ứng: **phần tử lớn nhất**) của X khi và chỉ khi a ≤ x (a ≥ x) với mọi x ∈ X.

• NHẬN XÉT:

a) Nếu tập được sắp (X, ≤) có phần tử bé nhất (phần tử lớn nhất) a thì a là phần tử bé nhất (tương ứng: lớn nhất) duy nhất. Thật vậy, giả sử còn có b là phần tử bé nhất thì ta suy ra a ≤ b và b ≤ a, từ đó, do tính phản xạ, a = b.

b) Một bộ phận A của tập được sắp (X, ≤) có thể có hoặc không có phần tử lớn nhất hoặc bé nhất. Chẳng hạn trong (3 , ≤), tập $\angle_0$ có phần tử bé nhất là 0, nhưng không có phần tử lớn nhất.

c) Một bộ phận A của tập được sắp (X, ≤) có thể không có phần tử cực đại, cực tiểu hoặc có một, hoặc có nhiều. Chẳng hạn: Trong (3 , ≤) bộ phận $\angle_0$ không có phần tử cực đại, đoạn [0, 1] có một phần tử cực đại và chỉ một, đó là 1 đó cũng

là phần tử lớn nhất của [0,1]; trong ($\angle$ – {1}, ξ) có vô số phần tử cực tiểu, đó là các số nguyên tố.

d) Nếu (X, $\leq$) được sắp thứ tự toàn phần thì X có nhiều nhất một phần tử cực đại, đó cũng là phần tử lớn nhất của X. Thật vậy, nếu a là phần tử cực đại của X. Lấy bất kì x thuộc X , vì $\leq$ là quan hệ thứ tự toàn phần nên ta có x $\leq$ a hoặc a $\leq$ x. Trong trường hợp a $\leq$ x, vì a là cực đại nên suy ra a = x. Vậy, ta luôn có x $\leq$ a với mọi x $\in$ X, tức là a là phần tử lớn nhất.

• Ta nói một tập hợp X là **sắp thứ tự tốt** nếu nó là sắp thứ tự và mọi bộ phận khác rỗng của X có một phần tử bé nhất. Chẳng hạn, ($\angle$, $\leq$) là tập được sắp tốt.

2. Cấu trúc đại số

2.1 Phép toán đại số

• Cho X và Y là hai tập khác $\varnothing$. **Phép toán trong** (hay **luật hợp thành trong**) **trên X** là một ánh xạ F : X x X $\rightarrow$ X. **Phép toán ngòai**(hay **luật hợp thành ngòai**) **trên X với tập toán tử Y** là ánh xạ G : Y x X $\rightarrow$ X. Phần tử F(x,y), G(x,y) được gọi là **cái hợp thành** của x và y.

• Người ta thường viết cái hợp thành của x và y bằng cách viết x và y theo một thứ tự nhất định với một dấu đặc trưng cho phép toán đặt giữa x và y. Chẳng hạn, F(x,y) = x + y, F(x,y) = x.y, F(x,y) = x$*$ y, F(x,y) = x $\perp$ y, …. Phép toán trong kí hiệu bằng dấu + được gọi là **phép cộng**, cái hợp thành x + y lúc này được gọi là **tổng của x và y**. Phép toán trong kí hiệu bằng dấu • được gọi là **phép nhân**, cái hợp thành x • y (đôi khi cũng được viết xy) lúc này được gọi là **tích của x và y**.

• VÍ DỤ:

a) Trên 9 các ánh xạ (x,y) $\mapsto$ xy; (x,y) $\mapsto$ x + y (phép nhân và cộng thông thường) là các phép toán trong. Ánh xạ (x,y) $\mapsto$ x $*$ y = 2x + 6xy + 5y cũng là phép toán trong trên 9. Tuy nhiên ánh xạ (x,y) $\mapsto$ x^y không phải là phép toán trên 9, vì nói chung x^y không thuộc 9.

b) Trên P(X) = {A : A $\subset$ X }, các ánh xạ (A, B) $\mapsto$ A $\cup$ B, (A, B) $\mapsto$ A $\cap$ B là các phép toán trong.

c) Trên tập M(X) = {f : X $\rightarrow$ X}, các ánh xạ từ X vào X, ánh xạ (f, g) $\mapsto$ f o g là phép toán trong

d) Đối với mỗi số thực x và số tự nhiên n, các ánh xạ (n, x) $\mapsto$ nx, (n,x) $\mapsto$ x^n là các phép toán ngòai trên 3 với tập toán tử $\angle$.

• Một phép toán $*$ trên một tập hữu hạn $X = \{x_1, x_2, \ldots, x_n\}$ thường được cho bằng cách trình bày dưới dạng một bảng. Trong bảng , người ta viết các phần tử của X ở bên trên và bên trái của bảng, dấu $*$ của phép toán được đặt ở góc trái phía trên. Trong phần giao của hàng thứ i và cột thứ j, người ta viết cái hợp thành $x_i * x_j$.

$*$	x_1	...	x_j	...	x_n
x_1	x_1*x_1	...	x_1*x_j	...	x_1*x_n
:	:	:	:	:	:
x_i	x_i*x_1	...	x_i*x_j	...	x_i*x_n
:	:	:	:	:	:
x_n	x_n*x_1	...	x_n*x_j	...	x_n*x_n

2.2 Các tính chất của phép toán đại số

Một phép toán $*$ trên tập X có thể thỏa mãn một số trong các tính chất sau đây:

• **Tính kết hợp** : $(a * b) * c = a * (b * c)$ với mọi $a, b, c \in X$

• **Tính giao hoán** : $a * b = b * a$ với mọi $a, b \in X$

• **Tính phân phối** : Giả sử $\perp$ là một phép toán khác trên X. Khi đó phép toán $*$ được gọi là

a) **phân phối trái** đối với $\perp$ nếu $a * (b \perp c) = a * b \perp a * c, \forall\ a, b, c \in X$
b) **phân phối phải** đối với $\perp$ nếu $(b \perp c) * a = b * a \perp c * a, \forall\ a, b, c \in X$
c) **phân phối** đối với phép toán $\perp$ nếu nó phân phối trái lẫn phân phối phải.

• **Thỏa luật giản ước :** Phép toán $*$ được gọi là thỏa mãn

a) **luật giản ước trái** nếu với mọi $a, b, c \in X$, từ $a * b = a * c$ kéo theo $b = c$
b) **luật giản ước phải** nếu với mọi $a, b, c \in X$, từ $b * a = c * a$ kéo theo $b = c$
c) **luật giản ước** nếu nó thỏa luật giản ước trái lẫn luật giản ước phải.

• VÍ DỤ:
1) Trong tập các số tự nhiên $\angle$, phép cộng và phép nhân thông thường có tính kết hợp, giao hoán, phép nhân phân phối đối với phép cộng; phép toán mũ hóa $(m, n) \mapsto m^n$ không giao hoán ($2^1 \neq 1^2$), không kết hợp ($(2^1)^2 \neq 2^{(1^2)}$).

2) Trong tập hợp các ánh xạ từ X vào X, phép toán hợp $g \circ f$ có tính kết hợp, không giao hoán (nếu X có nhiều hơn một phần tử)

2.3 Các phần tử đặc biệt

Cho tập hợp X và trên đó có một phép toán $*$.

• Phần tử $e \in X$ được gọi là

– **phần tử đơn vị trái** đối với phép toán $*$ nếu $e * a = a$, với mọi $a \in X$.
– **phần tử đơn vị phải** đối với phép toán $*$ nếu $a * e = a$, với mọi $a \in X$.
– **phần tử đơn vị** đối với phép toán $*$ nếu $e * a = a * e = a$, với mọi $a \in X$.

• Giả sử e là phần tử đơn vị đối với phép toán $*$ trên X. Phần tử $a' \in X$ được gọi là

– **nghịch đảo trái** của $x \in X$ nếu $a' * a = e$
– **nghịch đảo phải** của $x \in X$ nếu $a * a' = e$
– **nghịch đảo** của $x \in X$ nếu $a' * a = a * a' = e$

• CHÚ Ý:
1) Nếu đối với phép toán $*$ trên X có phần tử đơn vị trái e' và phần tử đơn vị phải e" thì e' = e". Điều này suy ra từ e' = e'$*$ e" = e" (đẳng thức thứ nhất do e" là đơn vị phải, đẳng thức thứ hai do e' là đơn vị trái).

Từ điều trên suy ra ngay lập tức rằng, đối với một phép toán trong có nhiều nhất là một phần tử đơn vị.

3) Phần tử đơn vị đối với phép cộng thường được kí hiệu bằng **0**, và phần tử nghịch đảo của x được kí hiệu là $-x$.
Phần tử đơn vị đối với phép nhân thường được kí hiệu bằng **1**, và phần tử nghịch đảo của x được kí hiệu là x^{-1}.

• VÍ DỤ:
1) Trong tập P(X) các tập con của X, phần tử đơn vị của phép toán $\cup$ là $e = \varnothing$, phần tử đơn vị của phép toán $\cap$ là e = X.

2) Trong 9, phần tử đơn vị của phép toán cộng thông thường là số 0, phần tử đơn vị của phép toán nhân thông thường là số 1.

3) Đối với phép toán hợp trên tập các ánh xạ từ X vào X, phần tử đơn vị là ánh xạ đồng nhất id_X.

2.4 Cấu trúc đại số

• Một bộ $(X, T_1, T_2, ..., T_n ; Y_1, \perp_1, Y_2, \perp_2, ..., Y_m, \perp_m)$ bao gồm tập hợp X khác $\varnothing$, các phép tóan trong T_i trên X ($1 \le i \le n$), các phép tóan ngòai $\perp_j$ trên X với tập tóan tử Y_j ($1 \le j \le m$) được gọi là một **cấu trúc đại số**.

• Giả sử $(X, T_1, T_2, ..., T_n ; Y_1, \perp_1, Y_2, \perp_2, ..., Y_m, \perp_m)$
và $(X', T'_1, T'_2, ..., T'_n ; Y_1, \perp'_1, Y_2, \perp'_2, ..., Y_m, \perp'_m)$ là hai cấu trúc đại số có cùng số lượng các phép toán trong, có cùng số lượng các phép toán ngòai với cùng các tập toán tử. Khi đó ánh xạ $f : X \to X'$ được gọi là một đồng cấu giữa hai cấu trúc đại số này nếu :

a) $f(a\ T_i\ b) = f(a)\ T'_i\ f(b)$, với mọi $a, b \in X$, với mọi $i = 1, 2, \ldots, n$.
b) $f(\alpha \perp_j b) = \alpha \perp'_j f(b)$, với mọi $\alpha \in Y_j$, $b \in X$, với mọi $j = 1, 2, \ldots, m$.

• Đồng cấu f được gọi là **đơn cấu, tòan cấu**, **đẳng cấu** nếu ánh xạ f tương ứng là đơn ánh, toàn ánh, song ánh.

2.5 Các cấu trúc đại số cơ bản

• Cấu trúc đại số $(X, *)$, trong đó $*$ là phép toán trong trên X, được gọi là

a) **nửa nhóm** nếu phép toán $*$ có tính chất kết hợp.
b) **vị nhóm** nếu phép toán $*$ có tính kết hợp, có phần tử đơn vị
c) **nhóm** nếu phép toán $*$ có tính kết hợp, có phần tử đơn vị, và mọi phần tử của X đều có nghịch đảo.

Nếu phép toán $*$ có tính giao hoán thì $(X, *)$ được gọi là **nhóm (vị nhóm, nửa nhóm) giao hoán**.

• Cấu trúc đại số $(X, +, \bullet)$, trong đó + và • là hai phép toán trong trên X, được gọi là một **vành** nếu:

a) (X, +) là một nhóm giao hoán.
b) $(X, \bullet)$ là một vị nhóm.
c) Phép toán • phân phối đối với phép +.

Phần tử đơn vị (kí hiệu là 1) của vị nhóm $(X, \bullet)$ cũng được gọi là **phần tử đơn vị của vành**. Nếu phép toán • có tính giao hoán thì vành $(X, +. \bullet)$ được gọi là **vành giao hoán**.

Cho $(X, +, \bullet)$ là một vành, nó có thể xảy ra trường hợp rằng, tồn tại các phần tử $a, b \in X$ sao cho $a \neq 0$, $b \neq 0$ (0 là phần tử đơn vị của nhóm (X,+)) nhưng $xy = 0$. Những phần tử như thế được gọi là **ước của không**. Một vành giao hoán, không có ước của không và $1 \neq 0$ được gọi là **vành nguyên** hoặc **miền nguyên**.

• Vành $(X, +, \bullet)$ được gọi là một **trường** nếu nó là giao hoán, phần tử đơn vị 1 khác 0, và mọi phần tử khác 0 dều có nghịch đảo đối với phép toán • .

• Cho (A, +, •) là một vành với phần tử đơn vị là 1. Cấu trúc đại số (M, +, •), trong đó + là phép toán trong trên M và • là phép toán ngòai trên M với tập toán tử A, được gọi là một **modul trên vành A** nếu :

a) (M, +) là một nhóm giao hoán.
b) Phép toán ngòai • thỏa các điều kiện sau

i) $\alpha(x + y) = \alpha x + \alpha y$ với mọi $\alpha \in A$, với mọi $x,y \in M$.
ii) $(\alpha+\beta)x = \alpha x + \beta x$
$(\alpha\beta)x = \alpha(\beta x)$ với mọi $\alpha, \beta \in A$, với mọi $x \in M$.
iii) $1x = x$ với mọi $x \in X$.

• Một modul trên một trường được gọi là là một **không gian vector** hay **không gian tuyến tính**.

BÀI TẬP

1. Chứng minh rằng :

1) $A \subset B \Rightarrow A \cap B = A$ và $A \cup B = B$
2) $A \cap B = A \Rightarrow A \subset B$
3) $A \cup B = B \Rightarrow A \subset B$

2. Cho X, Y là hai tập con của Z, hãy chứng tỏ

1) $Z - X \subset Z - Y \Leftrightarrow Y \subset X$
2) $(Z - Y) \cup Y = X \Leftrightarrow Y \subset X$

3. Chứng minh rằng : $(\bigcup_{k=1}^{n} A_k) - (\bigcup_{k=1}^{n} B_k) \subset (\bigcup_{k=1}^{n} (A_k - B_k))$.
Cho ví dụ chứng tỏ nói chung dấu '=' không xảy ra.

4. Chứng minh rằng với các tập hợp bất kì A, B, C thì

1) $A \times (B \cup C) = (A \times B) \cup (A \times C)$
2) $(A \cup B) \times C = (A \times C) \cup (B \times C)$
3) $A \times (B \cap C) = (A \times B) \cap (A \times C)$
4) $(A \cap B) \times C = (A \times C) \cap (B \times C)$

5. Xét tập hợp $\{A_1, A_2, \ldots\ldots, A_n\}$ mà các phần tử $A_1, A_2, \ldots\ldots, A_n$ là những tập hợp. Chứng minh rằng có ít nhất một tập hợp A_i không chứa một tập hợp nào trong các tập hợp còn lại.

6. Cho n_0 là một số tự nhiên. Xét tính đơn ánh, tòan ánh, song ánh của ánh xạ

$$f : \angle \to \angle,\ f(n) := \begin{cases} n_0 - n & \text{khi } n < n_0 \\ n_0 + n & \text{khi } n \geq n_0 \end{cases}$$

7. Cho $f : X \to Y$, $g : Y \to Z$ là các ánh xạ và $h = g \circ f$ là hợp của f và g, chứng minh:

1) Nếu h đơn ánh thì f đơn ánh
2) Nếu h đơn ánh và f tòan ánh thì g đơn ánh.
3) Nếu h là tòan ánh thì g là tòan ánh.
4) Nếu h tòan ánh và g đơn ánh thì f tòan ánh.

8. Cho ba ánh xạ $f : X \to Y$ và $g_1, g_2 : A \to X$, hãy chứng minh

1) Nếu f đơn ánh và $f \circ g_1 = f \circ g_2$ thì $g_1 = g_2$.

2) Nếu với mọi g_1, g_2 mà từ $fo\, g_1 = fo\, g_2$ kéo theo $g_1 = g_2$, thì f là đơn ánh.

9. Cho ba ánh xạ $f : X \to Y$ và $g_1, g_2 : Y \to A$, hãy chứng minh

1) Nếu f tòan ánh và $g_1 \circ f = g_2 \circ f$ thì $g = g'$.
2) Nếu với mọi g_1, g_2 mà $g_1 \circ f = g_2 \circ f$ kéo theo $g_1 = g_2$, thì f là tòan ánh.

10. Hãy thiết lập các song ánh giữa các tập hợp sau

1) Tập hợp các số tự nhiên và tập hợp các số tự nhiên chẵn.
2) Tập hợp các số tự nhiên và tập hợp các số nguyên chẵn.
3) Tập hợp các số hữu tỉ ở trong đọan [0, 1] và tập hợp các số tự nhiên .
4) Đoạn [0, 1] và đoạn [a, b]
5) Đoạn [0, 1] và nửa trục $[a, +\infty)$, $a > 0$.
6) Đoạn [0, 1] và khoảng (0, 1)

11. Chỉ ra rằng các tập hợp $\angle$ và $\angle \times \angle$, trong đó $\angle$ là tập hợp các số tự nhiên, có cùng lực lượng.

12. Cho E là một tập hợp, R là một quan hệ phản xạ trong E sao cho với mọi x, y, z $\in$ E, từ xRy và yRz kéo theo zRx. Chứng tỏ R là một quan hệ tương đương.

14. Cho E là một tập hợp, R là một quan hệ phản xạ và bắc cầu trong E. S là một quan hệ trong E xác định bởi x S y $\Leftrightarrow$ (xRy và yRx). Chứng tỏ R là một quan hệ tương đương.

14. Cho ánh xạ $f : 3 \to 3$, $f(x) = x^2 - x$. Trên 3 xác định một quan hệ S như sau x Sy $\Leftrightarrow$ f(x) = f(y). Chứng tỏ R là một quan hệ tương đương, và xác định lớp tương đương chứa phần tử x: $[x]_S$.

15. Cho một đơn ánh $f : X \to \angle$. Trên X xác định một quan hệ R như sau xRy $\Leftrightarrow f(x) \le f(y)$. Chứng tỏ R là quan hệ thứ tự toàn phần.

16. Xét tính kết hợp, giao hoán, tồn tại phần tử đơn vị trái - phải của phép toán $*$ trên tập hợp X.

1) $a * b = 2a + b - a^2$, X = 9

2) $a * b = \begin{cases} a + b & \text{khi } b \ge 0 \\ a & \text{khi } b < 0 \end{cases}$, X = 9

3) $a * b = \sqrt{a^2 + b^2}$, $X = (0, +\infty)$.

4) $a * b = a + b - ab,\ X = 3$

5) $a * b = e^{x+y},\ X = 3$

6) $a * b = a^b,\ X = \angle$

17. Cho X là một tập hợp mà trên đó có hai phép toán trong $*$ và $\perp$ với phần tử đơn vị tương ứng là e_0 và e. Ngòai ra phép toán $*$ phân phối trái đối với phép $\perp$ và phép toán $\perp$ phân phối trái đối với phép $*$. Chứng minh rằng $a * a = a$ và $a \perp a = a$ với mọi $a \in X$.

18. Phép nhân các số vô tỉ có phải là phép tóan trong trên tập các số vô tỉ không?

CHƯƠNG 2:
SỐ HỌC TRÊN 9

1. Số tự nhiên

1.1 Xây dựng số tự nhiên

• Ta xây dựng tập số tự nhiên bằng phương pháp tiên đề, đó là tập hợp $\angle$ cùng với ánh xạ $\sigma : \angle \to \angle$ thỏa mãn các tiên đề (gọi là tiên đề Peano) sau đây :

1) Có một phần tử kí hiệu là $1 \in \angle$.
2) $\sigma : \angle \to \angle^+ := \{n \in \angle : n \neq 1\}$ là một song ánh.

3) Nếu $\begin{cases} . \ S \subset IN \\ . \ 1 \in S \\ . \ \sigma(n) \in S \ \text{khi} \ n \in S \end{cases}$ thì $S = \angle$.

Tập $\angle$ với ánh xạ σ thỏa mãn các tiên đề trên được gọi là **tập số tự nhiên**, mỗi phần tử của nó được gọi là một **số tự nhiên**.
Người ta kí hiệu $\sigma(1) = 2,\ \sigma(2) = 3,\ \sigma(3) = 4,\ \sigma(4) = 5, \ldots$

• NHẬN XÉT:
a) Nếu ta kí hiệu $\sigma(n)$ bằng n^+ và hình dung n^+ như là " phần tử đứng liền sau phần tử n " thì tiên đề 2) nói rằng:
- $\sigma(n) \neq 1, n$, tức là, số 1 không đứng liền sau bất kì số tự nhiên nào.
- $\forall\ n \in \angle^+, \exists!\ m \angle : \sigma(m) = m^+ = n$, tức là mỗi số tự nhiên khác 1 đều đứng liền sau không quá một số tự nhiên.

b) Tiên đề 3) cho một phương pháp chứng minh gọi là phép chứng minh qui nạp. Nếu muốn chứng minh một tính chất E nào đó đúng với mọi số tự nhiên, thì trước hết ta chứng minh tính chất đó đúng cho số tự nhiên 1, sau đó chứng minh nó đúng cho số n^+ (số đứng liền sau số n), với " giả thiết qui nạp" rằng tính chất E đúng cho số n.

c) $m = n \Leftrightarrow m^+ = n^+$

1.2 Phép cộng trên $\angle$

• **Phép cộng** trên $\angle$ là ánh xạ $(n, m) \mapsto n + m$ thỏa mãn các tính chất sau

a) $n + 1 = n^+$ với mọi $n \in \angle$
b) $n + m^+ = (n + m)^+$ với mọi $n, m \in \angle$.

• Để định nghĩa phép cộng được đúng đắn, cần phải chỉ ra rằng tổng của hai số tự nhiên tồn tại và được xác định duy nhất.

Sự tồn tại. Đặt S = {n $\in \angle$: $\forall$ m $\in \angle$, $\exists$ ánh xạ (n,m)$\mapsto$ n + m thỏa a) và b)}
- Với n = 1, đặt 1 + m = m^+ thì rõ ràng rằng 1 $\in$ S.
- Giả sử n $\in$ S, tức là xác định được n + m với mọi m thỏa a) và b). Với n^+ nếu ta đặt $n^+ + m = (n + m)^+$ thì

$$n^+ + 1 = (n + 1)^+ = (n^+)^+ \quad \text{và} \quad n^+ + m^+ = (n + m^+)^+ = ((n + m)^+)^+ = (n^+ + m)^+$$

- Từ đó, $n^+ \in$ S, và theo tiên đề 3) thì S = $\angle$.

Sự duy nhất. Giả sử còn có phép toán (m,n)$\mapsto$ n $*$ m thỏa mãn các tính chất n $*$ 1 = n^+ và n $*$ m^+ = (n $*$ m)$^+$. Đặt S = {m $\in \angle$: n + m = n $*$ m, $\forall$ n $\in \angle$}. Vì n +1 = n^+ = n $*$ 1 nên 1 $\in$ S . Giả sử m $\in$ S, tức là n + m = n $*$ m, khi đó n $*$ m^+ = (n $*$ m)$^+$ = (n + m)$^+$ = n + m^+, suy ra $m^+ \in$ S. Từ đó, theo tiên đề 3) ta có S = $\angle$.

• NHẬN XÉT Trong chứng minh sự tồn tại của phép toán +, người ta đã định nghĩa 1 + m := m^+.

1.3 Định lí

($\angle$, +) là nửa nhóm giao hoán, thỏa luật giản ước.

Chứng minh:
• Tính kết hợp: Đặt S = {k $\in \angle$: m + (n + k) = (m + n) + k $\forall$n, m $\in \angle$}.
Ta có 1 $\in$ S, vì m + (n + 1) = m + n^+ = (m + n)$^+$ = (m + n) + 1.
Giả sử k $\in$ S,
khi đó
$$m + (n + k^+) = m + (n + k^+) = m + (n + k)^+$$
$$= (m + (n + k))^+ = ((m + n) + k)^+ = (m + n) + k^+.$$

Suy ra $k^+ \in$ S. Từ đó S = $\angle$.

• Tính giao hoán : Nếu đặt S = {m $\in \angle$: m + n = n + m, $\forall$ n $\in \angle$}
Ta có 1 $\in$S, vì 1 + n = n^+ = n + 1
Giả sử m $\in$ S,
khi đó
$$n + m^+ = (n + m)^+ = (m + n)^+ = m + n^+ = m + (1 + n)$$
$$= (m + 1) + n = m^+ + n.$$

Suy ra $m^+ \in$ S. Từ đó S = $\angle$.

• Thỏa luật giản ước : S = {k $\in \angle$: nếu n + k = m + k thì n = m }.
Ta có 1 $\in$S, vì nếu n + 1 = m + 1 thì $n^+ = m^+$, từ đó n = m.
Giả sử k $\in$ S và $n + k^+ = m + k^+$

khi đó $(n + k)^+ = (m + k)^+ \Rightarrow n + k = m + k \Rightarrow n = m$
Suy ra $k^+ \in S$. Từ đó $S = \angle$. □

1.4 Phép nhân trên $\angle$

• **Phép nhân** trên $\angle$ là ánh xạ $(n, m) \mapsto n \bullet m$ thỏa mãn các tính chất sau :

a) $n \bullet 1 = n$ với mọi $n \in \angle$
b) $n \bullet m^+ = n \bullet m + m$ với mọi $n, m \in \angle$

• Để định nghĩa phép nhân được đúng đắn, cần phải chỉ ra rằng tích của hai số tự nhiên tồn tại và được xác định duy nhất. Điều này được làm bằng cách tương tự như đã làm đối với phép cộng.

1.5 Định lí a) $(\angle, \bullet)$ là vị nhóm giao hoán, thỏa luật giản ước.
b) Phép nhân phân phối đối với phép cộng

Chứng minh: Chứng minh bằng phương pháp qui nạp tương tự như đối với phép cộng. Phần tử đơn vị là số 1. □

1.6 Quan hệ thứ tự trên tập hợp số tự nhiên

• Nếu với hai số m và n cho trước , có một số $k \in N$ sao cho $m = n + k$ thì ta nói rằng **m lớn hơn n** và viết **m > n**, khi đó ta cũng nói rằng **n bé hớn m** và viết **n < m**. Nếu **m lớn hơn hoặc bằng n** thì viết **m ≥ n**, nếu **n bé hơn hoặc bằng m** thì viết **n ≤ m**.

• Các quan hệ $\leq, <$ là các quan hệ thứ tự trên tập số tự nhiên $\angle$.

• Ta nói một nửa nhóm (vị nhóm, nhóm) $(X, *)$ là **nhóm (vị nhóm, nhóm) sắp thứ tự** (bộ phận, tòan phần, tốt, chặt, không chặt) nếu trên tập X đã xác định một quan hệ thứ tự (bộ phận, tòan phần, tốt, chặt, không chặt), $<$, sao cho

từ $x < y$ kéo theo $x * a < y * a$ và $a * x < a * y$ với mọi $a \in X$.

và X được gọi là **nhóm (vị nhóm, nhóm) sắp thứ tự mạnh** nếu thêm tính chất
từ $x * a < y * a$ hoặc $a * x < a * y$ kéo theo $x < y$, với mọi $a \in X$.

1.7 Định lí:

Với các quan hệ thứ tự $\leq, <$ nửa nhóm cộng $(\angle, +)$ và vị nhóm nhân $(\angle, \bullet)$ là được sắp thứ tự tòan phần, tốt và mạnh.

Chứng minh:
(chỉ chứng minh cho quan hệ $\leq$, đối với quan hệ $<$ cũng tương tự)

• *Sắp thứ tự toàn phần:* Với mọi $m \in \angle$, đặt $S = \{n \in \angle : n \leq m$ hoặc $m \leq n\}$.
Trước hết ta có $1 \in S$, thật vậy, nếu $m = 1$ thì điều đó là rõ ràng, nếu $m \neq 1$ thì $m = k^+ = k + 1$ với $k \in \angle$ nào đó, tức là $1 < m$, từ đó $1 \in S$.
Giả sử $n \in S$. Có ba khả năng xảy ra :
- Nếu $n = m$ thì $n^+ = m + 1$, từ đó $m \leq n^+$, tức là $n^+ \in S$.
- Nếu $n < m$ thì $m = n + k$ với $k \in \angle$ nào đó, thế thì $m = n + 1 = n^+$ hoặc $m = n + h^+ = (n + h)^+ = n^+ + h$ (với $h^+ = k$), từ đó $n^+ \leq m$, tức là $n^+ \in S$.
- Nếu $m < n$ thì $n = m + k$ với $k \in \angle$ nào đó, suy ra $n^+ = (m + k)^+ = m + k^+$, từ đó $m < n^+$, tức là $n^+ \in S$.
Tóm lại, trong mọi trường hợp đều có $n^+ \in S$. Vậy theo tiên đề 3) thì $S = \angle$.

• *Sắp thứ tự tốt:* Với mọi $A \subset \angle$, đặt $S = \{a \in \angle : a \leq x$ với mọi $x \in A\}$
Trước hết ta có $1 \in S$ và $S \neq \angle$ (vì nếu $x \in A$ thì do $x^+ > x$ nên $x^+ \notin S$).
Ta luôn tìm được một số $b \in S$ sao cho $b^+ \notin S$, vì nếu không, tức là với mọi $b \in S$ suy ra $b^+ \in S$, thì do tiên đề 3) ta có $S = \angle$. Số b này phải thuộc A. Thật vậy, nếu $b \notin A$ thì do $b \in S$ nên ta có $b < x$ với mọi $x \in A$. Từ đó $b^+ \leq x$ với mọi x thuộc A, tức là $b^+ \in S$. Nhưng điều này mâu thuẩn với $b^+ \notin S$. Như vậy, ta đã chỉ ra rằng, tồn tại số $b \in A$ sao cho $b \leq x$ với mọi $x \in A$, nghĩa là b là phần tử bé nhất của A.

• *Sắp thứ tự mạnh:* Ta sẽ chứng minh các khẳng định sau

$$a \leq b \Leftrightarrow a + c \leq b + c, \text{ với mọi } c \in \angle$$
$$a \leq b \Leftrightarrow ac \leq bc, \quad \text{với mọi } c \in \angle$$

- Giả sử $a \leq b$. Nếu $a = b$ thì rõ ràng $a + c = b + c$, $ac = bc$. Nếu $a < b$ thì ta có $b = a + k$ với $k \in \angle$ nào đó. Khi đó
$b + c = (a + k) + c = (a + c) + k \Rightarrow a + c < b + c$
$bc = (a + k)c = ac + kc \Rightarrow ac < bc$.

- Giả sử $a + c \leq b + c$ (tương ứng $ac \leq bc$). Nếu $b < a$ thì theo chứng minh chiều thuận, $b + c < a + c$ (tương ứng $bc < ac$). Điều này dẫn đến mâu thuẩn.□

2. Vành số nguyên

2.1 Xây dựng tập số nguyên

• Xét tập $\angle \times \angle = \{(m, n) : m, n \in \angle\}$ gồm mọi cặp số tự nhiên. Trên tập $\angle \times \angle$ đưa vào một quan hệ tương đương như sau:

$$(m, n) \sim (p, q) \Leftrightarrow m + q = n + p.$$

• Ta kí hiệu [m, n] là lớp tương đương của (m,n) và 9 là tập thương của $\angle$ x$\angle$ đối với quan hệ ~ . 9 được gọi là là **tập các số nguyên**, mỗi phần tử cuả nó gọi là một **số nguyên**.

2.2 Phép cộng

• Phép cộng giữa hai số nguyên [m, n] và [p, q] được xác định bởi

$$[m, n] + [p, q] = [m + p, n + q]$$

• Để định nghĩa được hợp lí, cần phải chỉ ra rằng định nghĩa trên không phụ thuộc vào việc chọn đại diện của [m, n]và [p, q], tức là phải chứng minh rằng, nếu (m, n) ~ (m', n') và (p, q) ~ (p', q') thì (m + p, n + q) ~ (m' + p', n' + q'). Thật vậy, theo định nghĩa: $m + n' = n + m'$ và $p + q' = q + p'$,
từ đó, $(m + p) + (n' + q') = (n + q) + (m' + p')$. Lại từ định nghĩa suy ra điều phải chứng minh.

2.3 Phép nhân

• Phép nhân giữa hai số nguyên [m, n] và [p, q] được xác định bởi

$$[m, n] \bullet [p, q] = [m p + n q, m q + n p]$$

• Để định nghĩa được hợp lí, cũng cần phải chỉ ra rằng định nghĩa trên không phụ thuộc vào việc chọn đại diện của [m, n]và [p, q] . Giả sử (m, n) ~ (m', n') và (p, q) ~ (p', q'). Khi đó $m + n' = n + m'$ (1) và $p + q' = q + p'$ (2)

Nhân (1) và (2) vế theo vế: **mp** + mq' + n'p + n'q' = nq + np' + m'q + **m'p'**
Nhân (1) với q **nq** + m'q = **mq** + n'q
Nhân (2) với n nq + np' = **np** + nq'
Nhân (1) với q' **m'q'** + nq' = mq' + **n'q'**
Nhân (2) với n' **n'p'** + n'q = n'p + n'q'

Cộng các đẳng thức vừa tìm được vế theo vế ta có:

$$mp + nq + m'q' + n'p' = mq + np + m'p' + n'q',$$

Tức là $(mp + nq, mq + np) \sim (m'p' + n'q', m'q' + n'p')$.

2.4 Định lí

(9 , +, •) là một vành, hơn nữa là một miền nguyên .

Chứng minh:

• Đối với phép cộng phần tử đơn vị là lớp có dạng [a, a], phần tử nghịch đảo của [m, n] là [n, m]. Đối với phép nhân phần tử đơn vị có dạng [1 + a, a]. Các tính chất khác của phép tóan cộng và nhân để làm cho (9 , +, •) là một vành chỉ là một sự kiểm tra đơn giản nhờ định nghĩa của các phép tóan và các tính chất đã biết đối với tập số tự nhiên.

• Giả sử [m, n]• [p, q] = 0 = [a, a], tức là (mp + nq, mq + np) ~ (a, a). Khi đó ta có mp + nq + a = mq + np + a, hay mp + nq = mq + np (1). Nếu [m, n] ≠ 0, tức là m ≠ n, thì ta sẽ chỉ ra [p, q] = 0. Giả sử m < n (đối với m > n cũng tương tự), khi đó n = m + k với k $\in \angle$ nào đó và đẳng thức (1) trở thành

$$mp + (m + k)q = mq + (m + k)p$$

hay

$$mp + mq + kq = mq + mp + kp,$$

từ đó, do luật giản ước đối với phép cộng và phép nhân các số tự nhiên ta có q = p, tức là [p, q] = 0. Điều này suy ra trên 9 không có ước của không. □

• NHẬN XÉT:

a) Nếu đặt $9_{>0} = \{ [n + a, a] : a, n \in \angle\} \subset 9$ thì $(9_{>0} , +)$ là một nửa nhóm cộng và từ đẳng cấu $\varphi : \angle \to 9_{>0}$, $n \mapsto [n + a, a]$, có thể đồng nhất $\angle$ với $9_{>0}$, tức là một số tự nhiên $n \in \angle$ được đồng nhất với lớp tất cả các cặp dạng (n + a, a) với a chạy qua tập hợp $\angle$.

b) Một số nguyên bất kì [m, n] đều có thể viết dưới dạng :

$$[m, n] = \begin{cases} [n + k, n] & \text{khi } m < n \\ [m, m + l] & \text{khi } m > n \\ [m, m] & \text{khi } m = n \end{cases}$$

Như vậy, các số nguyên có thể chia làm ba loại : **số không** (là lớp tương đương của các cặp dạng (a, a) , khi đó ta viết [a, a] = 0), **số nguyên dương** (là lớp có dạng [m, n] với m > n, khi đó ta viết [m, n] > 0), **số nguyên âm** (là lớp có dạng [m, n] với m < n, khi đó ta viết [m, n] < 0).

Nếu đặt – n = [a, n + a] thì vành số nguyên có thể viết dưới dạng

$$9 = \{.... – 3, – 2, – 1, 0, 1, 2, 3,.....\} .$$

2.5 Quan hệ thứ tự trên 9

• Trên 9 có thể xác định phép tóan trừ như sau :

$$\begin{aligned}[a, b] - [c, d] &= [a, b] + (-[c, d]) \\ &= [a, b] + [d, c]) \\ &= [a + d, b + c]\end{aligned}$$

• Bây giờ trên vành số nguyên ta xác định một quan hệ thứ tự lớn hơn " > " như sau

$$\begin{aligned}[a, b] > [c, d] &\Leftrightarrow [a, b] - [c, d] > 0. \\ &\Leftrightarrow [a + d, b + c] > 0 \\ &\Leftrightarrow a + d > b + c\end{aligned}$$

Ta có thể kiểm tra dễ dàng đó là một quan hệ thứ tự trên 9.

Ở trên ta đã trình bày cách xây dựng tập số nguyên từ tập số tự nhiên. Từ định nghĩa các phép toán và quan hệ thứ tự có thể thấy lại các qui tắc cũng như các tính chất thông thường của số nguyên mà ta đã quen biết.

3. Sự chia hết trên tập số nguyên

3.1 Định nghĩa

• Cho a, b là hai số nguyên . Ta nói rằng **a chia hết b** (hoặc **a là ước của b**, hoặc **b chia hết cho a**, hoặc **b là bội của a**), ký hiệu $a \mid b$ nếu tồn tại một số nguyên c sao cho $b = ac$.

• Rõ ràng là $a \mid 0$ với mọi số nguyên a, và $0 \mid a$ khi và chỉ khi $a = 0$

3.2 Tính chất (a, b, c, d là các số nguyên)

1) $\pm a \mid a$ và $\pm 1 \mid a$.
2) Nếu $a \mid 1$ thì $a = \pm 1$
3) Nếu $a \mid b$ và $b \mid a$ thì $a = \pm b$.
4) Nếu $a \mid b$ và $b \mid c$ thì $a \mid c$
5) Nếu $a \mid b$ thì $a \mid bc$
6) Nếu $a \mid b$ và $a \mid c$ thì $a \mid b + c$
7) Nếu $a \mid b$ và $c \mid d$ thì $ac \mid bd$
8) Nếu $a \mid b$ thì $a^n \mid b^n$ (n là số tự nhiên)
9) Nếu $a \mid b_i$, $\forall\, i = 1, 2, \ldots, n$ thì $a \mid \sum_{i=1}^{n} m_i b_i$ (b_i, m_i là các số nguyên)

Chứng minh: Việc chứng minh chỉ là sự kiểm tra đơn giản từ định nghĩa. □

3.3 Định lí (phép chia Euclide)

Cho a, b là hai số nguyên với $b \neq 0$. Khi đó tồn tại duy nhất một cặp số nguyên q, r sao cho $a = b\,q + r$ với $0 \le r < |b|$.

(q gọi là **thương** và r gọi là **dư** của phép chia a cho b)

Chứng minh:

• *Sự tồn tại*. Đặt $S = \{n \in 9 : n|b| \le a\} \subset 9$, khi đó S khác ∅ vì $-|a| \in S$.
S bị chặn trên nên có phần tử lớn nhất k. Do $k|b| \le a$ nên $a = k|b| + r$; với $r \ge 0$. Mặt khác, vì $k = \max S$ nên $k+1 \notin S$, tức là, $(k+1)|b| > a$. Từ đó suy ra $k|b| + |b| > k|b| + r$ hay $r < |b|$.

Nếu đặt $q = \begin{cases} k & \text{khi } b > 0 \\ -k & \text{khi } b < 0 \end{cases}$ thì $k|b| = qb$, và từ những điều đã trình bày ở trên ta có $a = bq + r$ với $0 \le r < |b|$.

• *Sự duy nhất*. Giả sử $a = bq + r$; $a = bq' + r'$ với $0 \le r, r' < |b|$. Khi đó ta có $r - r' = b(q' - q)$. Vì $|r - r'| < |b|$ nên $|b||q' - q| < |b|$ hay $|q' - q| < 1$. Từ đó $q' = q$ và $r = r'$. □

3.4 Ước chung lớn nhất (ƯCLN)

• Số nguyên c được gọi là **ước chung** của n số nguyên $a_1, a_2, ..., a_n$ nếu c là ước của a_i với mọi i = 1, 2, …, n.

• Số nguyên c được gọi là **ước chung lớn nhất** của n số nguyên $a_1, a_2, ..., a_n$ khi và chỉ khi d là ước chung của $a_1,...,a_n$ và nếu c là ước chung bất kỳ của $a_1,...,a_n$ thì c là ước d.

• NHẬN XÉT:
a) Nếu d_1 và d_2 là các ước chung lớn nhất của $a_1, a_2, ..., a_n$ thì $d_1 = \pm d_2$.
Người ta thường viết $(a_1, a_2, ..., a_n)$ để chỉ **ước chung lớn nhất không âm** của n số nguyên $a_1, a_2, ..., a_n$.

b) Rõ ràng rằng ƯCLN của 0 và b là b.

3.5 Định lí

Ước chung lớn nhất của n số nguyên bất kì $a_1, a_2, ..., a_n$ luôn luôn tồn tại.

Chứng minh :

Nếu $a_1 = a_2 = ... = a_n = 0$ thì rõ ràng $(a_1, a_2, ..., a_n) = 0$. Giả sử $a_1, a_2, ..., a_n$ không đồng thời bằng không.

Đặt $I = \{y \in 9 : y = \sum_{i=1}^{n} x_i a_i , x_i \in 9 , i = 1,2,\ldots,n\}$ và $J = \{|y| : y \in I\} - \{0\}$.

Vì $a_1, a_2, ..., a_n$ không đồng thời bằng 0 nên $I \neq \{0\}$ và từ đó $J \neq \emptyset$. Do J bị chặn dưới, nên J có số nhỏ nhất. Giả sử $|d| = \min J$ với $d = \sum_{i=1}^{n} x_i a_i \in I$. Ta sẽ chứng minh d là ước chung lớn nhất của $a_1,..., a_n$. Thật vậy, với mỗi i ta có $a_i = dq_i + r_i$; $0 \leq r_i < |d|$. Suy ra

$r_i = a_i - dq_i = (-x_1q_i)a_1 + ... + (-x_{i-1}q_i)a_{i-1} + (1 - x_i q_i)a_i + ... + (-x_nq_i)a_n$.

Từ đó $r_i \in I$ với mọi i = 1, 2, …, n. Ta phải có $r_i = 0$ vì nếu không thì $r_i \in J$ và điều này mâu thuẩn với |d| là số nhỏ nhất của J. Từ đó suy ra d là ước chung của $a_1,...,a_n$. Mặt khác nếu c là ước chung bất kỳ của $a_1,...,a_n$ thì c là ước của $\sum_{i=1}^{n} x_i a_i$ tức là c là ước của d. Vậy d là ƯCLN của $a_1,..., a_n$. □

3.6 Hệ quả

a) Nếu e là ước chung lớn nhất của $a_1, a_2,..., a_n$ thì tồn tại $x_1, x_2, ...,x_n \in 9$ sao cho $e = x_1a_1 + x_2a_2 + ... + x_na_n$.

b) Nếu e là ước chung của $a_1, a_2,..., a_n$ và tồn tại $x_1, x_2, ...,x_n \in 9$ sao cho $e = x_1a_1 + x_2a_2 + ... + x_na_n$ thì e là ước chung lớn nhất của $a_1, a_2,..., a_n$.

Chứng minh:

a) Xét ước chung lớn nhất d của $a_1, a_2,..., a_n$ trong chứng minh định lí 1.5. Vì $e = \pm d$ nên ta có điều phải chứng minh.

b) Giả sử c là ước chung bất kỳ của $a_1,...,a_n$ thì c là ước của $\sum_{i=1}^{n} x_i a_i$ tức là c là ước của e. Vậy e là ƯCLN của $a_1,..., a_n$. □

3.7 Định lí

d là ước chung lớn nhất của $a_1, a_2, ..., a_n$ khi và chỉ khi d là ước chung lớn nhất của $(a_1,...,a_{n-1})$ và a_n.

Chứng minh :

Giả sử $d = (a_1 ,. . ., a_n)$, $d_1 = ((a_1 ,. . ., a_{n-1}), a_n)$ và $m = (a_1 ,. . ., a_{n-1})$. Vì d là ước của a_i với mọi i = 1, 2, …, n nên d là ƯC của m và a_n ; nhưng d_1 là ƯCLN của m và a_n nên d là ước của d_1. Mặt khác d_1 là ƯC của m và a_n nên d_1 là ƯC của của a_i với mọi i = 1, 2, …, n và do d là là ƯCLN của a_i với mọi i = 1, 2, …, n nên d_1 là ước d. Từ đó $d_1 = d$. □

3.8 Định lí

Giả sử a, b, q, r là những số nguyên thỏa mãn hệ thức a = bq + r. Khi đó ƯCLN của a và b cũng là ƯCLN của b và r.

Chứng minh: Nếu đặt d = (a, b) thì d | a và d | b, nhưng vì r = a – bq nên ta cũng có d | r và d | b. Giả sử c là một ƯC bất kì của b và r, khi đó vì a = bq + r nên c cũng là ƯC của b và a, vậy c phải là ước của d. Từ đó d = (b, r). □

3.9 Thuật toán tìm ƯCLN của hai số

Giả sử muốn tìm ƯCLN của hai số nguyên a và b. Nếu a = 0 thì rõ ràng ƯCLN của a và b là b, vì vậy ta chỉ xét cho trường hợp cả a lẫn b đều khác 0. Thuật toán là một quá trình thực hiện liên tiếp các phép chia:

• Bước 1: Chia a cho b $a = bq_0 + r_0$ với $0 \le r_0 < |b|$.
Nếu $r_0 = 0$ thì dừng. Nếu $r_0 \ne 0$ thì đi đến bước 2

• Bước 2: Chia b cho r_0 $b = r_0q_1 + r_1$ với $0 \le r_1 < r_0$.
Nếu $r_1 = 0$ thì dừng. Nếu $r_2 \ne 0$, thì đi đến bước 3
. . . . . .

• Bước n : Chia r_{n-1} cho r_n $r_{n-1} = r_n q_{n+1} + r_{n+1}$ với $0 \le r_{n+1} < r_n$.

Quá trình chia như vậy phải chấm dứt sau một số hữu hạn bước vì dãy các số tự nhiên $|b| > r_0 > \ldots > r_i > \ldots \ge 0$ không thể giảm vô hạn. Giả sử đến bước n nào đó ta có $r_{n+1} = 0$ và $r_n \ne 0$, thì theo định lí 3.8 suy ra ƯCLN của a và b là r_n.

• VÍ DỤ: Tìm ƯCLN của 9100 và 1848

Giải: Ta sắp xếp các phép chia liên tiếp như sau:

	4	1	12	5
9100 :	1848 :	1708 :	140 :	28
1708	140	28	0	

Từ đó (9100, 1848) = 28.

4. Số nguyên tố cùng nhau.

4.1 Định nghĩa

• Các số nguyên $a_1, a_2, ..., a_n$ được gọi là **nguyên tố cùng nhau** nếu chúng nhận số 1 làm ƯCLN.

• Ta nói rằng các số nguyên $a_1, a_2, ..., a_n$ **nguyên tố cùng nhau từng đôi** nếu và chỉ nếu $(a_i, a_j) = 1$ với mọi $i \neq j$.

• NHẬN XÉT:
1) Nếu các số nguyên $a_1, a_2, ..., a_n$ nguyên tố cùng nhau từng đôi thì chúng là nguyên tố cùng nhau, vì khi đó

$$(a_1, a_2, a_3, ..., a_n) = ((a_1, a_2), a_3, ..., a_n) = (1, a_3, ..., a_n) = 1$$

Điều ngược lại nói chung không đúng, chẳng hạn $a_1 = 3, a_2 = 10, a_3 = 15$.

2) Nếu $(a, b) = 1$ và $c \mid b$ thì $(a, c) = 1$. Thật vậy, nếu $d \in \angle$ và $(d \mid a, d \mid c)$ thì $(d \mid a, d \mid b)$, vậy $d = 1$. Từ đó suy ra $(a, c) = 1$.

4.2 Định lí (Bezout)

Điều kiện cần và đủ để các số nguyên $a_1, a_2, ..., a_n$ nguyên tố cùng nhau là tồn tại các số nguyên $x_1, x_2, ..., x_n$ sao cho $\sum_{i=1}^{n} x_i a_i = 1$.

Chứng minh: Suy ra trực tiếp từ hệ quả 1.6 □

4.3 Định lí (Gauss)

Nếu các số nguyên a, b, c thỏa mãn $a \mid bc$ và $(a, b) = 1$ thì $a \mid c$.

Chứng minh: Giả sử $(a, b) = 1$ và $a \mid bc$. Theo định lí Bezout, tồn tại hai số nguyên x và y sao cho $ax + by = 1$. Suy ra $c = axc + byc$. Vì $a \mid axc$ và $a \mid byc$ nên $a \mid c$. □

4.4 Định lí

Cho $x, a_1, a_2, \ldots, a_n$ là các số nguyên khác 0. Khi đó

$$((x, a_i) = 1, \text{ với mọi } i \in \{1, 2, \ldots, n\}) \Leftrightarrow (x, \prod_{i=1}^{n} a_i) = 1$$

Chứng minh:
($\Rightarrow$) Ta chứng minh bằng cách qui nạp theo n. Với $n = 1$ thì khẳng định là hiển nhiên. Đối với $n = 2$, giả sử $(x, a_1) = (x, a_2)$. Theo định lí Bezout, tồn tại $u_1, v_1, u_2, v_2 \in 9$ sao cho $xu_1 + a_1v_1 = 1$ và $xu_2 + a_2v_2 = 1$. Khi đó $(x, a_1 a_2) = 1$ vì

$$1 = (xu_1 + a_1v_1)(xu_2 + a_2v_2) = x(x\, u_1\, u_2 + a_1\, v_1\, u_2 + u_1\, a_2\, v_2) + (a_1\, a_2)(v_1\, v_2)$$

Vậy, khẳng định đúng với n = 2. Bây giờ, giả thiết khẳng định đúng với n và giả sử $a_1, a_2, \ldots, a_{n+1} \in 9$ sao cho $(x, a_i) = 1$, với mọi $i \in \{1, 2, \ldots, n, n+1\}$. Thế thì $(x, a_i) = 1$, với mọi $i \in \{1, 2, \ldots, n\}$ và theo giả thiết qui nạp, $(x, \prod_{i=1}^{n} a_i) = 1$, rồi theo kết quả khảo sát cho trường hợp n = 2 ta có

$$(x, \prod_{i=1}^{n+1} a_i) = (x, \prod_{i=1}^{n} a_i . a_{n+1}) = 1$$

($\Leftarrow$) Nếu $(x, \prod_{i=1}^{n} a_i) = 1$ thì theo nhận xét 2) trong mục 4.1 suy ra $(x, a_i) = 1$. □

5 Bội chung nhỏ nhất (BCNN)

5.1 Định nghĩa :

• Số nguyên c được gọi là một **bội chung** của n số nguyên $a_1,\ldots,a_n$ nếu $a_i \mid c$ với mọi i = 1, 2, …, n.

• Số nguyên d được gọi là **bội chung nhỏ nhất** (BCNN) của n số nguyên $a_1,\ldots,a_n$ khi và chỉ khi d là bội chung của $a_1,\ldots,a_n$ và nếu c là một bội chung bất kì của $a_1,\ldots,a_n$ thì $d \mid c$.

• NHẬN XÉT:
1) Nếu d_1, d_2 là các bội chung nhỏ nhất của $a_1,\ldots,a_n$ thì $d_1 = \pm d_2$. Vậy bội chung nhỏ nhất của $a_1,\ldots,a_n$ là duy nhất theo nghĩa sai khác dấu. Ta dùng kí hiệu $[a_1,\ldots,a_n]$ để chỉ bội chung nhỏ nhất không âm của $a_1,\ldots,a_n$.
2) BCNN của 0 và b là 0.

5.2 Mệnh đề

$(a, b)[a, b] = |ab|$ với mọi $a, b \in 9$

Chứng minh:
Nếu a = 0 hoặc b = 0 thì hiển nhiên. Vậy ta chỉ chứng minh cho trường hợp a và b đều khác 0, khi đó $(a,b) \neq 0$. Nếu đặt $m = \frac{|ab|}{(a,b)}$ thì m là một bội chung của a và b. Gọi t là một bội chung bất kì của a và b. Vì $a \mid t$ nên tồn tại $c \in 9$ sao cho t = ac, từ đó $\frac{t}{(a,b)} = \frac{ac}{(a,b)}$. Vì $b \mid t$ nên $\frac{b}{(a,b)}$ cũng là ước của $\frac{t}{(a,b)}$, và do đó $\frac{b}{(a,b)}$ là ước của $\frac{ac}{(a,b)}$. Nhưng $\frac{a}{(a,b)}$ và $\frac{b}{(a,b)}$ là nguyên tố cùng nhau nên

theo định lí Gauss(4.3) suy ra $\frac{b}{(a,b)}$ là ước của c. Vậy $\frac{ab}{(a,b)}$ là ước của ac = t, từ đó m | t, tức là m = [a, b] □

• NHẬN XÉT: Từ mệnh đề 5.2 suy ra nếu a và b là nguyên tố cùng nhau thì ab là BCNN của a và b.

5.3 Mệnh đề

BCNN của n số nguyên $a_1,...,a_n$ luôn luôn tồn tại và

$$[a_1,...,a_n] = [[a_1,...,a_{n-1}], a_n] .$$

Chứng minh (Ta chứng minh bằng quy nạp.)

• n = 2 (do 5.2)

• Giả sử tồn tại $m_{n-1} = [a_1,...,a_{n-1}]$. Đặt $m = [m_{n-1}, a_n]$. Vì m là bội chung của m_{n-1} và a_n nên m là bội chung của $a_1,...,a_n$. Giả sử t là bội chung của $a_1,...,a_n$. Hiển nhiên t là bội chung của $a_1,...,a_{n-1}$, do đó t là bội của m_{n-1} và a_n . Vì m là BCNN của m_{n-1} và a_n nên t là bội của m. Vậy $m = [a_1,...,a_n]$ □

6. Số nguyên tố

Để đơn giản, các khái niệm và kết quả trong phần này ta chỉ trình bày trên tập các số nguyên dương ∠. Các khái niệm và kết quả đó cũng có thể chuyển lên tập các số nguyên 9.

6.1 Định nghĩa

• Một số tự nhiên khác 1 gọi là **số nguyên tố** nếu nó chỉ chia hết cho 1 và cho chính nó . Một số tự nhiên khác 1 và không phải là số nguyên tố được gọi là **hợp số.** Ta có thể nói số nguyên n là số nguyên tố nếu | n | là số nguyên tố.

• CHÚ Ý : Số 1 không phải là số nguyên tố cũng không phải là hợp số.

6.2 Định lí

Ước số dương nhỏ nhất khác 1 của một số tự nhiên lớn hơn 1 là một số nguyên tố.

Chứng minh: Xét $a \in \angle$ và a >1. Gọi p là ước số dương nhỏ nhất khác 1 của a. Nếu p không phải là nguyên tố thì p là hợp số, nên p có một ước số là p_1 với :1 < p_1 < p. Nhưng khi đó p_1 cũng là ước số của a, và điều này mâu thuẫn với tính nhỏ nhất của p. □

6.3 Định lí

Tập các số nguyên tố trong ∠ là vô hạn .

Chứng minh: Giả sử ngược lại, $\angle$ chỉ có một số hữu hạn các số nguyên tố là p_1 ,..., p_n . Từ 6.3 suy ra số tự nhiên $M = p_1 ... p_n + 1$ có ước số dương nhỏ nhất khác 1 là một số nguyên tố p. Như thế tồn tại $j \in \{1, 2, \ldots, n\}$ sao cho $p = p_j$, do đó $p \mid p_1 ... p_n$. Từ đó $p \mid (M - p_1 ... p_n)$ hay $p \mid 1$ (mâu thuẩn) □

6.4 Định lí

Cho $a \in \angle$ và p là số nguyên tố. Khi đó hoặc $(a, p) = 1$ hoặc $p \mid a$.

Chứng minh: Vì (a, p) là một ước của p, nên nó chỉ có thể là p hoặc là 1. Nếu $(a, p) \neq 1$ thì $(a, p) = p$, nhưng khi đó $p \mid a$. □

6.5 Định lí

Giả sử $a_1,...,a_n \in \angle$ và p là số nguyên tố. Khi đó hai điều sau đây là tương đương

1) p là ước của $\prod_{i=1}^{n} a_i$

2) Tồn tại $i \in \{1, 2, \ldots, n\}$ sao cho $p \mid a_i$.

Chứng minh:

$(1 \Rightarrow 2)$ Giả sử $p \mid \prod_{i=1}^{n} a_i$. Nếu p không là ước của các a_i, với mọi i, thì theo 6.4 suy ra $(p, a_i) = 1$, với mọi i. Từ đó, theo định lí 4.4, $(p, \prod_{i=1}^{n} a_i) = 1$, vậy $p = 1$, và điều đó dẫn đến mâu thuẩn.

$(2 \Rightarrow 1)$ là hiển nhiên □

6.6 Định lí

Ước số dương nhỏ nhất khác 1 của một hợp số $a > 1$ là một số nguyên tố nhỏ hơn hoặc bằng $\sqrt{a}$.

Chứng minh: Giả sử ước số đó là p, khi đó p là nguyên tố và $a = pa_1$.Vì a_1 là một ước dương khác của a nên $a_1 \geq p$, thế thì $a = pa_1 \geq p^2$.Vậy $p \leq \sqrt{a}$ □

6.7 Sàng Eratosthène

Để lập bảng số nguyên tố không vượt quá một số nguyên dương n, ta có thể áp dụng một phương pháp gọi là sàng Eratosthen. Nội dung của phương pháp này như sau :

• Lập dãy số 1, 2, 3, 4, …, n
(Số thứ nhất lớn hơn 1 của dãy số trên là 2, hiển nhiên 2 là số nguyên tố)
• Trong dãy số trên, ta xóa tất cả các bội của 2.
(Số thứ nhất đứng sau 2 không bị xóa là 3. Hiển nhiên 3 là số nguyên tố)
• Tiếp tục ta xóa tất cả các bội của 3.
. . . . . .

• Cứ tiếp tục theo cách đó, ta xóa tất cả các bội số của các số nguyên tố nhỏ hơn một số nguyên tố p, thì tất cả các số không bị xóa nhỏ hơn p^2 đều nguyên tố. Thật vậy, mọi hợp số a nhỏ hơn p^2 đều đã bị xóa vì là bội của ước số dương nhỏ nhất của nó, ước số này, theo 6.6, nhỏ hơn $\sqrt{a} < p$.

Suy ra rằng :
1) Khi xóa các bội của một số nguyên tố p, thì số đầu tiên bị xóa là p^2.
2) Khi đã xóa các bội của các số nguyên tố $\leq \sqrt{n}$ thì hoàn thành việc lập bảng.

• VÍ DỤ: Nếu n = 50 thì ta chỉ xóa các bội của các số nguyên tố 2,3,5,7.

6.8 Định lí (cơ bản của số học)

Mọi số tự nhiên lớn hơn 1 đều phân tích được thành tích những thừa số nguyên tố, và sự phân tích này là duy nhất nếu không kể đến thứ tự các nhân tử.

Chứng minh
1) *Sự tồn tại.* Xét $a \in \angle$ và $a > 1$.
Gọi p_1 là ước số nguyên tố nhỏ nhất của a. Ta có

$$a = p_1a_1 \text{ với } 1 \leq a_1 < a.$$

Nếu $a_1 = 1$ thì $a = p_1$ (chứng minh xong).
Nếu $a_1 > 1$, gọi p_2 là ước số nguyên tố nhỏ nhất của a_1 . Ta có

$$a_1 = p_2a_2 \text{ với } 1 \leq a_2 < a_1 .$$

Nếu $a_2 = 1$ thì $a = p_1p_2$ (chứng minh xong).
Nếu $a_2 > 1$, lặp lại lý luận trên cho các bước sau . . . . . .

Quá trình này phải kết thúc sau một số hữu hạn bước vì ta có :

$$a > a_1 > a_2 > \ldots > 1.$$

Giả sử quá trình kết thúc ở bước thứ n, với $a_n = 1$. Khi đó $a = p_1p_2...p_n$.

2) *Sự duy nhất.* Giả sử $p_1p_2...p_n = a = q_1q_2...q_m$, trong đó, các p_i , q_j là các số nguyên tố. Khi đó $p_1 \mid q_1...q_m$ và tồn tại $j \in \{1, 2, \ldots, m\}$ sao cho $p_1 = q_j$ (xem 6.5). Bằng cách đánh số lại, ta có thể giả sử $p_1 = q_1$. Giản ước ta có $p_2...p_n = q_2...q_m$.

Nếu $m > n$ thì bằng cách thực hiện tiếp tục quá trình trên . ta được $1 = q_{n+1}...p_m$, nhưng điều này không thể xảy ra được vì các q_j là các số nguyên tố. Vậy

phải có $m \le n$. Vì vai trò của m và n là như nhau, nên ta cũng có $n \le m$. Từ đó $m = n$ và $p_i = q_i$ với mọi i. Vậy phân tích là duy nhất theo nghĩa sai khác nhau về thứ tự các nhân tử.

6.9 Dạng phân tích chính tắc.

• Khi phân tích một số tự nhiên $a > 1$ thành tích các nhân tử nguyên tố, một vài hoặc tất cả các nhân tử nguyên tố đó có thể giống nhau. Kết hợp các nhân tử giống nhau lại và biểu diễn tích của chúng dưới dạng lũy thừa thì sẽ dẫn đến dạng sau gọi là dạng phân tích chính tắc $a = p_1^{k_1} p_2^{k_2} \ldots p_m^{k_m}$.

• VÍ DỤ: $9100 = 2^2.5^2.7.13$; $128 = 2^7$.

6.10 Định lí

Cho một số tự nhiên a vơí dạng phân tích chính tắc $a = p_1^{k_1} p_2^{k_2} \ldots p_m^{k_m}$.
Khi đó, một số tự nhiên d là ước của a khi và chỉ khi d có dạng :

$$d = p_1^{r_1} p_2^{r_2} \ldots p_m^{r_m} \quad \text{với} \quad 0 \le r_i \le k_i \,, i = 1, 2, \ldots, m.$$

Chứng minh:
• Giả sử d | a, tức là a = dq. Đẳng thức này chứng tỏ mọi ước số nguyên tố của d đều có mặt trong a với số mũ của nó trong d không vượt quá số mũ của nó trong a.

• Giả sử a và d có dạng như trên, ta có

$$a = p_1^{k_1} p_2^{k_2} \ldots p_m^{k_m} = p_1^{r_1} p_2^{r_2} \ldots p_m^{r_m} (p_1^{k_1 - r_1} p_2^{k_2 - r_2} \ldots p_m^{k_m - r_m})$$

Đẳng thức này chứng tỏ d | a. □

• VÍ DỤ: Cho $a = 60 = 2^2. 3. 5.$ Các ước của a có dạng $d = 2^x. 3^y. 5^z$. Cho x lần lượt các giá trị 0, 1, 2; cho y lần lượt các giá trị 0,1 và z lần lượt là 0, 1 thì ta sẽ được tất cả các ước của a, chẳng hạn với x = 2, y = 1, z = 0 ta có một ước của a = 60 là d = 4.

6.11 Cách tìm ƯCLN và BCNN

• Cho hai số tự nhiên a và b có khai triển thừa số nguyên tố dạng chính tắc :
$a = p_1^{k_1} p_2^{k_2} \ldots p_m^{k_m}$ và $b = p_1^{t_1} p_2^{t_2} \ldots p_m^{t_m}$, trong đó k_i và t_i có thể bằng 0, khi đó

$$(a, b) = p_1^{\min(k_1,t_1)} \times p_2^{\min(k_2,t_2)} \times \ldots \times p_m^{\min(k_m,t_m)}$$

$$[a, b] = p_1^{\max(k_1,t_1)} \times p_2^{\max(k_2,t_2)} \times \ldots \times p_m^{\max(k_m,t_m)}$$

• VÍ DỤ:

$9100 = 2^2 . 5^2 . 7 . 13 = 2^2 . 3^0 . 5^2 . 7^1 . 11^0 . 13^1$
$1848 = 2^2 . 3 . 7 . 11 = 2^2 . 3^1 . 5^0 . 7^1 . 11^1 . 13^0$
$(9100, 1848) = 2^2 \times 3^0 \times 5^0 \times 7^1 . 11^0 . 13^0 = 28$
$[9100, 1848] = 2^2 \times 3^1 \times 5^2 \times 7^1 \times 11^1 \times 13^1$

7 Đồng dư

7.1 Định nghĩa

• Cho m là một số tự nhiên lớn hơn 1, và a, b là hai số nguyên. Nói rằng a **là đồng dư modulo m với** b (hoặc **a đồng dư với b theo modulo m**) nếu trong phép chia a và b cho m ta được cùng một số dư. Nếu a đồng dư với b theo modulo m thì ta viết $a \equiv b \pmod m$ và gọi hệ thức này là **đồng dư thức modulo m**.

• Ta có các dạng tương đương khác của định nghĩa đồng dư:

1) $a \equiv b \pmod m \Leftrightarrow m \mid (a - b)$
2) $a \equiv b \pmod m \Leftrightarrow a = b + mk$ với $k \in 9$

Thật vậy, ta chứng minh chẳng hạn 1). Nếu $a \equiv b \pmod m$ thì theo định nghĩa ta có $a = m q_1 + r$ và $b = m q_2 + r$. Từ đó, $a - b = m(q_1 - q_2)$, tức là $m \mid (a - b)$. Ngược lại, nếu $m \mid (a - b)$, tức là $a - b = m q$. Giả sử $b = mq_1 + r$ với $0 \leq r < m$ khi đó ta có $a = mq + b = mq + mq_1 + r = m(q + q_1) + r$. Điều này chứng tỏ khi chia a và b cho m thì có cùng số dư r.

7.2 Lớp đồng dư

• Quan hệ đồng dư modulo m là một quan hệ tương đương trên 9. Thật vậy, tính phản xạ và đối xứng là hiển nhiên. Giả sử $a \equiv b \pmod m$ và $b \equiv c \pmod m$, khi đó $m \mid (a - b)$ và $m \mid (b - c)$, suy ra $m \mid (a - b) + (b - c)$, tức là $m \mid (a - c)$, vậy $a \equiv c \pmod m$ và do đó có tính bắc cầu.

• Ta kí hiệu $9/_{m9}$ là tập thương của 9 theo quan hệ (tương đương) đồng dư modulo m. Với mọi $x \in 9$, ta kí hiệu lớp tương đương chứa của x trong $9/_{m9}$ là $\bar{x}$ hay [x]. Nhờ phép chia Euclide cho m : $x = mq + r$, $0 \leq r \leq m - 1$, ta thấy rằng mỗi số nguyên x đều đồng dư modul m với $r \in \{0, 1, 2, \ldots, m - 1\}$. Hơn nữa các số thuộc $\{0, 1, 2, \ldots, m - 1\}$ không đồng dư với nhau theo modulo m, do đó có đúng m lớp

đồng dư theo modulo m, mà ta có thể chọn các số trên làm đại diện cho mỗi lớp, $\mathbb{Z}/m\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{m-1}\}$.

7.3 Tính chất

Tính chất 1: Có thể cộng, trừ, nhân vế theo vế các đồng dư thức của cùng modulo:

Nếu $a_i \equiv b_i \pmod m$, $i = 1, 2, \ldots, k$ thì $\sum_{i=1}^{k} a_i \equiv \sum_{i=1}^{k} b_i \pmod m$

Nếu $a_i \equiv b_i \pmod m$, $i = 1, 2, \ldots, k$ thì $\prod_{i=1}^{k} a_i \equiv \prod_{i=1}^{k} b_i \pmod m$

Chứng minh: Theo định nghĩa $a_i = b_i + mt_i$, và khẳng định được suy ra từ $\sum_{i=1}^{k} a_i = \sum_{i=1}^{k} b_i + m\sum_{i=1}^{k} t_i$ và $\prod_{i=1}^{k} a_i = \prod_{i=1}^{k} b_i + m\,Q$. □

Tính chất 2: Các khẳng định dưới đây là hệ quả trực tiếp của tính chất 1

a) Nếu $a \equiv b \pmod m$ thì $a \pm c \equiv b \pm c \pmod m$
b) Nếu $a \equiv b \pmod m$ thì $a + km \equiv b \pmod m$
c) Nếu $a \equiv b \pmod m$ thì $a^n \equiv b^n \pmod m$

• VÍ DỤ: Tìm tất cả các số nguyên $p \geq 2$ sao cho p và $2^p + p^2$ là những số nguyên tố.

Giải: Rõ ràng p = 2 không thích hợp và p = 3 là thỏa mãn yêu cầu đề ra. Nếu p là số nguyên tố ≥ 5 thì ta có $2^p \equiv (-1)^p \pmod 3$ và $p^2 \equiv 1 \pmod 3$. Từ đó suy ra $2^p + p^2 \equiv 0 \pmod 3$. Vì $2^p + p^2$ là nguyên tố nên ta có Vì $2^p + p^2 = 3$, nhưng điều này là không thể. Như vậy số p cần tìm là p = 3.

BÀI TẬP

1. Chứng minh rằng nếu k là một số nguyên dương và $a_1, a_2, \ldots, a_n$ là n số nguyên thì

$$(ka_1, ka_2, \ldots, ka_n) = k(a_1, a_2, \ldots, a_n)$$

2. Chứng minh rằng nếu số nguyên dương c là ước chung của n số nguyên $a_1, a_2, \ldots, a_n$ thì

$$\left(\frac{a_1}{c}, \frac{a_2}{c}, \ldots, \frac{a_n}{c}\right) = \frac{1}{c}(a_1, a_2, \ldots, a_n)$$

3. Cho a, b, c là ba số nguyên, chứng minh rằng

a) Nếu (a, c) = 1 và (b, c) = 1 thì (ab, c) = 1
b) $(a, b) = 1 \Leftrightarrow (a^n, b^n) = 1$ với $n \in \angle$
c) $(a^n, b^n) = (a, b)^n$ với $n \in \angle$

4. Chứng minh rằng
$n^2 \equiv 0 \pmod 8$ hoặc $n^2 \equiv 4 \pmod 8$ nếu n là số nguyên chẵn
$n^2 \equiv 1 \pmod 8$ nếu n số nguyên lẻ

5. Chứng minh rằng nếu $n \geq 1$ thì $2^{2^n} \equiv 1 \pmod 3$

6. Cho a là một số nguyên lẻ và $n \geq 3$ là một số tự nhiên. Chứng minh rằng

$$a^{2^{n-1}} \equiv 1 \pmod{2^n}$$

7. Chứng minh rằng với mọi số tự nhiên n thì $\sum_{k=1}^{2n} \frac{(2n)!}{k}$ là một số nguyên chia hết cho 2n + 1.

8. Tìm tất cả các số nguyên n sao cho

a) $21 \mid (2^{2n} + 2^n + 1)$
b) $7 \mid (2^{2^n} + 2^n + 1)$
d) $10 \mid n^2 + (n^2 + 1)^2 + (n^2 + 3)^2$
e) $8 \mid 3^n + 4n + 1$

9. a) Cho $a, x_1, x_2, \ldots, x_n \in 9$. Chứng minh rằng, nếu $x_1, x_2, \ldots, x_n$ là nguyên tố cùng nhau từng đôi và $x_i \mid a$ với mọi i = 1, 2, …, n thì $\prod_{i=1}^{n} x_i \mid a$.

b) Nếu $x_1, x_2, \ldots, x_n$ là nguyên tố cùng nhau từng đôi thì

$$[x_1, x_2, \ldots, x_n] = |\prod_{i=1}^{n} x_i|$$

10. Định lí Trung hoa về phần dư

a) Cho $a_1, a_2, \ldots, a_n \in \angle$ là nguyên tố cùng nhau từng đôi và $a = \prod_{i=1}^{n} a_i$. Chứng minh rằng với mọi số nguyên $b_1, b_2, \ldots, b_n$ tồn tại một số nguyên β sao cho

$$\begin{cases} x \equiv b_i (\mathrm{mod}\, a_i) \\ x \in Z, i = 1,2,...,n \end{cases} \Leftrightarrow x \equiv \beta \ (\mathrm{mod}\ a)$$

b) Giải trong 9 phương trình sau

$$\begin{cases} x \equiv 4(\mathrm{mod}\, 5) \\ x \equiv 3(\mathrm{mod}\, 6) \\ x \equiv 2(\mathrm{mod}\, 7) \end{cases}$$

11. Chứng minh rằng các số nguyên sau là hợp số.

a) $n^4 - n^2 + 16$ với $n \in 9$
b) $4n^3 + 6n^2 + 4n + 1$ với $n \in \angle$
c) $2^{4n+2} + 1$ với $n \in \angle$
d) $5^n - 3^n$ với $n \in \angle$ và $n \geq 2$.
e) $a^n + b^n + c^n + d^n$ với $a, b, c, d \in \angle$ và $ab = cd$

12. Tìm tất cả các số nguyên $n \geq 2$ sao cho n và $n^3 + n^2 + 11n + 2$ là những số nguyên tố.

13. Cho $p \geq 3$ là số nguyên tố, $n \in \angle$. Chứng minh rằng

$$(1 + p)^{p^n} \equiv 1 + p^{n+1} (\mathrm{mod}\ p^{n+2})$$

14. Cho $a, b \in \angle$ sao cho $\frac{1}{2}(a^3 + b^3)$ là một số nguyên tố. Chứng tỏ $a = b = 1$.

15. Cho $n \in \angle$ sao cho $n \geq 11$. Chứng minh rằng nếu $n - 10, n + 10, n + 60$ là những số nguyên tố thì thì $n + 90$ cũng là số nguyên tố.

16. Tìm tất cả các số nguyên tố có dạng $2^{2^n} + 5, n \in \angle$.

17. Định lí nhỏ Fermat :Cho p là số nguyên tố

a) Chứng minh : Với mọi $n \in 9$, $n^p \equiv n(\mathrm{mod}\ p)$
b) Suy ra: Với mọi $n \in 9$, $(p \mid n \Rightarrow n^{p-1} \equiv 1(\mathrm{mod}\ p)$

18. Chứng minh rằng với mọi số nguyên n, số $\frac{n^7}{7} + \frac{n^5}{5} + \frac{23n}{35}$ là một số nguyên.

19. Chứng minh, với mọi $n \in 9$

a) $42 \mid n^7 - n$

b) $2730 \mid n^{13} - n$

c) $2^{15}-2^3 \mid n^{15} - n^3$

20. Chứng minh rằng

a) Với mọi số nguyên lẻ $n \geq 15$, $21840 \mid n^{12}-1$

b) Với mọi số nguyên tố $p \geq 19$, $16320 \mid p^{16}-1$.

CHƯƠNG 3: NHÓM

1 Nửa nhóm - Vị nhóm

1.1 Định nghĩa

• Cấu trúc đại số $(X, *)$ với $*$ là phép toán trong trên X có tính chất kết hợp được gọi là **nửa nhóm**. Một nửa nhóm có phần tử đơn vị được gọi là **vị nhóm**. Một nửa nhóm là **giao hoán** nếu phép toán trên nó có tính giao hoán.

• VÍ DỤ:

1) Tập số tự nhiên $\angle$ với phép toán cộng thông thường là một nửa nhóm giao hoán. Tập số tự nhiên(với số 0) $\angle_0$ với phép toán cộng thông thường là một vị nhóm giao hoán.

2) Tập số tự nhiên $\angle$ với phép toán $a * b = (a, b)$ (ƯCLN của a và b) là một nửa nhóm giao hoán.

3) Tập P(X) các tập con của X cùng với phép toán $\cup$ (hoặc $\cap$) là vị nhóm giao hoán.

4) Tập M(X) các ánh xạ từ X vào X với phép tóan hợp các ánh xạ là một vị nhóm không giao hoán.

1.2 Tích của n phần tử trong nửa nhóm

• Trong nửa nhóm $(X. \bullet)$ **tích của n phần tử $a_1, a_2, ..., a_n$** của X được xác định bằng qui nạp như sau:

$$a_1 \bullet a_2 \bullet a_3 = (a_1 \bullet a_2) \bullet a_3$$
$$a_1 \bullet a_2 \bullet a_3 \bullet a_4 = (a_1 \bullet a_2 \bullet a_3) \bullet a_4$$
$$. \ . \ . \ . \ . \ . \ . \ . \ . \ . \ . \ . \ . \ . \ .$$
$$a_1 \bullet a_2 \bullet \ldots \bullet a_{n-1} \bullet a_n = (a_1 \bullet a_2 \bullet \ldots \bullet a_{n-1}) \bullet a_n.$$

• Tích của n phần tử $a_1, a_2, \ldots, a_n$ còn được kí hiệu là $\prod_{i=1}^{n} a_i$. Nếu nửa nhóm (X,+) được viết theo lối cộng thì ta viết dấu tổng thay vì dấu tích:

$$\sum_{i=1}^{n} a_i = a_1 + a_2 + \ldots + a_{n-1} + a_n = (a_1 + a_2 + \ldots + a_{n-1}) + a_n$$

1.3 Định lí

Giả sử $a_1, a_2, \ldots, a_n$ là n phần tử bất kì của nửa nhóm $(X, \bullet)$. Khi đó

$$a_1 \bullet a_2 \bullet \ldots \bullet a_{n-1} \bullet a_n = (a_1 \bullet \ldots \bullet a_i) \bullet (a_{i+1} \bullet \ldots \bullet a_j) \bullet \ldots \bullet (a_{m+1} \bullet \ldots \bullet a_n)$$

Chứng minh: Ta sẽ chứng minh định lí trên bằng phương pháp qui nạp theo n. Vì (X, •) là nửa nhóm nên khẳng định đúng với n = 3. Giả sử khẳng định đúng cho k phần tử ,với $3 \le k \le n-1$, ta phải chứng minh khẳng định đúng với n phần tử phần tử . Xét tích $x = (a_1 \bullet \ldots \bullet a_i) \bullet (a_{i+1} \bullet \ldots \bullet a_j) \bullet \ldots \bullet (a_{m+1} \bullet \ldots \bullet a_n)$ ta có

$x = (a_1 \bullet \ldots \bullet a_m) \bullet (a_{m+1} \bullet \ldots \bullet a_n)$ (giả thiết qui nạp)
$= (a_1 \bullet \ldots \bullet a_m) \bullet [(a_{m+1} \bullet \ldots \bullet a_{n-1}) \bullet a_n]$ (định nghĩa của tích nhiều phần tử)
$= [(a_1 \bullet \ldots \bullet a_m) \bullet (a_{m+1} \bullet \ldots \bullet a_{n-1})] \bullet a_n$ (tính kết hợp)
$= (a_1 \bullet \ldots \bullet a_m \bullet a_{m+1} \bullet \ldots \bullet a_{n-1}) \bullet a_n$ (giả thiết qui nạp)
$= a_1 \bullet a_2 \bullet \ldots \bullet a_{n-1} \bullet a_n$ (định nghĩa của tích nhiều phần tử)

Từ đó khẳng định đúng với n phần tử . □

• Trong nửa nhóm (X. •) ta gọi tích của n phần tử đều bằng a **là lũy thừa n của phần tử a** và kí hiệu là a^n. Từ định lí 1.2 suy ra ngay các qui tắc:

$$a^m \, a^n = a^{m+n} \text{ và } (a^m)^n = a^{mn}$$

1.4 Định lí

Trong một nửa nhóm giao hoán (X, •) tích $a_1 \bullet a_2 \bullet \ldots \bullet a_{n-1} \bullet a_n$ không phụ thuộc vào thứ tự các nhân tử.

Chứng minh: Ta sẽ chứng minh định lí trên bằng phương pháp qui nạp theo n. Vì (X, •) là nửa nhóm giao hoán nên khẳng định đúng với n = 2. Giả sử khẳng định đúng cho k phần tử ,với $2 \le k \le n-1$, ta phải chứng minh khẳng định đúng với n phần tử. Ta sẽ chỉ ra (với σ là hoán vị bất kì của 1, 2, …, n)

$$a_1 \bullet a_2 \bullet \ldots \bullet a_{n-1} \bullet a_n = a_{\sigma(1)} \bullet a_{\sigma(2)} \bullet \ldots \bullet a_{\sigma(n)}$$

Nếu $a_n = a_{\sigma(k)}$ thì ta có thể viết vế phải của đẳng thức trên như sau nhờ định lí 1.3 và tính giao hoán của phép toán • :

$a_{\sigma(1)} \ldots a_{\sigma(k-1)} a_{\sigma(k)} a_{\sigma(k+1)} \ldots a_{\sigma(n)} = (a_{\sigma(1)} \ldots a_{\sigma(k-1)}) [a_{\sigma(k)} (a_{\sigma(k+1)} \ldots a_{\sigma(n)})]$

(do $a_n = a_{\sigma(k)}$ và tính giao hoán) $= (a_{\sigma(1)} \ldots a_{\sigma(k-1)}) [(a_{\sigma(k+1)} \ldots a_{\sigma(n)}) a_n]$

(do tính kết hợp) $= [(a_{\sigma(1)} \ldots a_{\sigma(k-1)})(a_{\sigma(k+1)} \ldots a_{\sigma(n)})] a_n.$

(do định lí 1.3) $= (a_{\sigma(1)} \ldots a_{\sigma(k-1)} a_{\sigma(k+1)} \ldots a_{\sigma(n)}) a_n.$

(theo giả thiết qui nạp) $= (a_1.a_2. \ldots . a_{n-1}).a_n = a_1.a_2. \ldots . a_{n-1}.a_n$ □

2 Nhóm

2.1 Định nghĩa

• Vị nhóm $(X, *)$ được gọi là một **nhóm** nếu mỗi phần tử của X đều tồn tại phần tử nghịch đảo. Hay nói cách khác, cấu trúc đại số $(X, *)$ được gọi là một nhóm nếu :

a) $(x * y) * z = x * (y * z)$ với mọi $x, y, z \in X$

b) Tồn tại phần tử $e \in X$ sao cho $e * x = x * e = x$ với mọi $x \in X$

c) Với mọi $x \in X$ tồn tại $y \in X$ sao cho $x * y = y * x = e$.

• VÍ DỤ:

1) Tập các số hữu tỉ Θ với phép cộng thông thường là một nhóm. Tập các số hữu tỉ khác 0, kí hiệu Θ^*, với phép nhân thông thường là một nhóm. Tập các số thực và số phức $3, \forall$ với phép cộng thông thường là các nhóm. Tập các số thực và số phức khác 0, kí hiệu $3^*, \forall^*,$ với phép nhân thông thường là các nhóm.

2) Tập hợp các số phức có modul bằng 1 với phép nhân thông thường là một nhóm.

3) Tập hợp gồm hai số $1, -1$ với phép nhân là một nhóm. Tập hợp gồm bốn số $1, -1, i, -i$ với phép nhân là một nhóm.

4) Với $X \neq \varnothing$, tập S(X) các song ánh từ X vào X là một nhóm dưới phép toán hợp các ánh xạ. Nhóm này được gọi là nhóm **các hoán vị của tập X.**

5) Cho $\{(X_I, \bullet)\}_{i\in I}$ là một họ các nhóm. Đặt $X = \prod_{i\in I} X_i = \{(x_i)_{i\in I} : x_i \in X_i\}$ là tích Descartes của họ $\{X_i\}_{i\in I}$.Với $(x_i)_{i\in I}$ và $(y_i)_{i\in I}$ là hai phần tử của X, ta xác định tích của chúng bởi : $(x_i)_{i\in I} \bullet (y_i)_{i\in I} = (x_I \bullet y_i)_{i\in I}$. Khi đó $(X, \bullet)$ là một nhóm, trong đó phần tử đơn vị là $1 = (1_{X_i})_{i\in I}$ và phần tử nghịch đảo của $(x_i)_{i\in I}$ là $(x_i^{-1})_{i\in I}$. Ta gọi X là **tích Descartes hay tích trực tiếp của họ các nhóm** $\{(X_i, \bullet)\}_{i\in I}$.

• Một nhóm gồm chỉ một phần tử được gọi là **nhóm tầm thường**. Một nhóm nói chung có thể có vô hạn hoặc hữu hạn phần tử . Nếu X có hữu hạn phần tử thì ta nói X là **nhóm hữu hạn**, và số phần tử của X được gọi là **cấp của nhóm X**. Các nhóm trong ví dụ 3) là các nhóm hữu hạn cấp hai và cấp 4. Nếu phép toán trên X có tính giao hoán thì ta nói X là **nhóm giao hoán** hay **nhóm abel**. Nhóm trong ví dụ 4) là nhóm không giao hoán.

• Trong một nhóm nhân $(X, \bullet)$ người ta có thể nói đến lũy thừa của một phần tử với số mũ là một số nguyên bất kì bằng cách đặt:

$$a^n = \begin{cases} a^n & \text{khi } n > 0 \\ 1 & \text{khi } n = 0 \\ (a^{-1})^{-n} & \text{khi } n < 0 \end{cases}$$

2.2 Các tính chất cơ bản của nhóm

Tính chất 1: Phần tử đơn vị của một nhóm là duy nhất.

Chứng minh:
Giả sử nhóm (X, •) có hai phần tử đơn vị là 1 và 1^* thì $1 = 1 \bullet 1^* = 1^*$. □

Tính chất 2: Mỗi phần tử của nhóm chỉ có duy nhất một phần tử nghịch đảo.

Chứng minh: Giả sử phần tử a của nhóm (X, •) có hai phần tử nghịch đảo là b và b^* thì $b = 1 \bullet b = (b^* \bullet a) \bullet b = b^* \bullet (a \bullet b) = b^* \bullet 1 = b^*$. □

Tính chất 3: Trong một nhóm luật giản ước thực hiện được với mọi phần tử, tức là từ đẳng thức $a \bullet b = a \bullet c$ hoặc $b \bullet a = c \bullet a$ kéo theo $b = c$.

Chứng minh: Giả sử a, b, c là các phần tử của nhóm (X, •) thỏa mãn đẳng thức a b = a c. Nhân bên trái hai vế của đẳng thức này với a^{-1}, ta có
$a^{-1}(a\ b) = a^{-1}(a\ c)$, hay $(a^{-1}a)\ b = (a^{-1}a)\ c$, hay $1b = 1c$, tức là $b = c$. □

Tính chất 4: Trong nhóm (X,•) ta có

1) $(a\ b)^{-1} = b^{-1}\ a^{-1}$, hoặc tổng quát hơn, $(a_1\ a_2\ \dots\ a_{n-1}\ a_n)^{-1} = a_n^{-1}\ a_{n-1}^{-1} \dots a_2^{-1}\ a_1^{-1}$, và đặc biệt, $(a^n)^{-1} = (a^{-1})^n$, trong đó $n \in \angle$.

2) $a^n\ a^m = a^{n+m}$ và $(a^n)^m = a^{n\,m}$ với mọi n, m $\in 9$.

Chứng minh:
1) Vì $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aa^{-1} = 1$
$(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b^{-1} = b^{-1}b = 1$

2) Nếu n = 0 hoặc m = 0 là hiển nhiên. Nếu n, m > 0 , các công thức được suy ra rừ định lí 1.2. Nếu m , n < 0 thì

$$a^n\ a^m = (a^{-1})^{-n}(a^{-1})^{-m} = (a^{-1})^{(-n)+(-m)} = (a^{-1})^{-(n+m)} = a^{n+m}$$

$(a^n)^m = [(a^{-1})^{-n}]^m = [(a^{-n})^{-1}]^m = (a^{-n})^{-m} = a^{nm}$.

Nếu $m < 0 < n$ thì

$(a^n)^m = ((a^n)^{-1})^{-m} = ((a^{-1})^n)^{-m} = (a^{-1})^{n(-m)} = (a^{-1})^{-nm} = a^{nm}$

$$a^n a^m = \begin{cases} a^{n+m}a^{-m}(a^{-m})^{-1} & \text{khi } n+m \geq 0 \\ a^n(a^{-1})^n(a^{-1})^{-m-n} & \text{khi } n+m < 0 \end{cases} = a^{n+m}.$$

□

Tính chất 5:
Cho $(X, \bullet)$ là một nửa nhóm. Khi đó ba điều sau đây là tương đương:

1) $(X, \bullet)$ là một nhóm.
2) Với mọi phần tử a, b của X, phương trình $ax = b$ cũng như phương trình $ya = b$ có nghiệm duy nhất.
3) Trong X tồn tại phần tử đơn vị trái (tương ứng: đơn vị phải) và mọi phần tử của X đều có nghịch đảo trái(tương ứng: nghịch đảo phải).

Chứng minh:
$(1 \Rightarrow 2)$ Ta thấy ngay giá trị $x = a^{-1}b$ là nghiệm của phương trình. Đó là nghiệm duy nhất vì nếu c cũng là nghiệm của phương trình, tức là $ac = ax = b$ thì $c = x$.
$(2 \Rightarrow 3)$ Gọi e là nghiệm của phương trình $ya = a$. Ta sẽ chỉ ra e là phần tử đơn vị trái. Thật vậy, với mọi phần tử b bất kì của X , nếu gọi c là nghiệm của phương trình $ax = b$, thì ta có $eb = e(ac) = (ea)c = ac = b$.
Giả sử a là một phần tử bất kì của X, khi đó phần tử nghịch đảo trái của a là nghiệm của phương trình $ya = e$.

$(3 \Rightarrow 1)$ Giả sử trong X tồn tại phần tử đơn vị trái e và mọi phần tử của X đều có nghịch đảo trái. Lấy một phần tử bất kì a của X. gọi a^{-1} là nghịch đảo trái của a và $(a^{-1})^{-1}$ là nghịch đảo trái của a^{-1}. Khi đó ta có

$$aa^{-1} = e(aa^{-1}) = ((a^{-1})^{-1}a^{-1})(aa^{-1}) = (a^{-1})^{-1}(a^{-1}a)a^{-1} = (a^{-1})^{-1}(ea^{-1})$$
$$= (a^{-1})^{-1}a^{-1} = e.$$

Mặt khác, với mọi phần tử b của X, gọi b^{-1} là nghịch đảo trái (và cũng là nghịch đảo phải) của b thì ta có : $be = b(b^{-1}b) = (bb^{-1})b = eb = b$.

Vậy, e là phần tử đơn vị của X và a^{-1} là phần tử nghịch đảo của a và do đó X là một nhóm. □

3. Nhóm con

3.1 Định nghĩa

• Cho $(X, \bullet)$ là một nhóm , và H là một tập con của X. H được gọi là **ổn định** (đối với phép toán • trong X) nếu và chỉ nếu $a \bullet b \in H$ với mọi $a, b \in H$. Khi đó người ta cũng nói rằng, phép toán trên X **cảm sinh một phép toán** trên H.

• Ta nói một bộ phận ổn định H của nhóm X là một **nhóm con của X** nếu H cùng với phép toán cảm sinh là một nhóm.

CHÚ Ý: Nếu H là nhóm con của nhóm $(X, \bullet)$ thì phần tử đơn vị của X là 1_X nằm trong H. Thật vậy, gọi 1_H là phần tử đơn vị của nhóm $(H, \bullet)$. Khi đó ta có $1_H \bullet 1_H = 1_H$ và $1_H \bullet 1_X = 1_H$, từ đó suy ra $1_H \bullet 1_H = 1_H \bullet 1_X$, và do luật giản ước trong nhóm ta có $1_X = 1_H \in H$.

3.2 Định lí (tiêu chuẩn để nhận biết một nhóm con)

Giả sử H là một tập con khác $\varnothing$ của một nhóm $(X, \bullet)$. Khi đó ba điều sau đây là tương đương:

1) H là một nhóm con của X.
2) $ab \in H$ và $a^{-1} \in H$ với mọi $a, b \in H$.
3) $ab^{-1} \in H$ với mọi $a, b \in H$.

Chứng minh:

$(1 \Rightarrow 2)$ Vì H là bộ phận ổn định của nhóm X nên $ab \in H$ với mọi $a, b \in H$. Xét a là một phần tử bất kì của H , giả sử a_H^{-1} là phần tử nghịch đảo của a trong H và a_X^{-1} là nghịch đảo của a trong X. Khi đó $a_H^{-1}.a = 1_H = 1_X = a_X^{-1}a$, và do luật giản ước trong nhóm ta có $a_X^{-1} = a_H^{-1} \in H$.

$(2 \Rightarrow 3)$ Điều này là rõ ràng.

$(3 \Rightarrow 1)$ Vì $H \neq \varnothing$ nên tồn tại phần tử $a \in H$, từ đó theo giả thiết $1_X = aa^{-1} \in H$. Với mọi $b \in H$, gọi b_X^{-1} là phần tử nghịch đảo của b trong X, từ $1_X \in H$ và từ giả thiết suy ra $b_X^{-1} = 1_X.b_X^{-1} \in H$. Bây giờ với mọi $a, b \in H$, khi đó $b^{-1} \in H$ và do giả thiết $ab = a(b^{-1})^{-1} \in H$. Điều này chứng tỏ • cũng là phép toán trên H, và do phép toán đã cho trong X có tính kết hợp nên $(H. \bullet)$ là nửa nhóm. Ngòai ra H có phần tử đơn vị là $1_H := 1_X$ và phần tử $a \in H$ có phần tử nghịch đảo là $a_H^{-1} := a_X^{-1}$. Từ đó $(H, \bullet)$ là một nhóm. □

• VÍ DỤ:

1) Cho nhóm $(X, \bullet)$. Bộ phận $\{1_X\}$ và X là hai nhóm con của nhóm X, chúng được gọi là các **nhóm con tầm thường** của nhóm X

2) $(\Theta, +)$ là nhóm con của $(3, +)$. Nhóm các số phức có modul bằng 1 là nhóm con của nhóm nhân $(\forall^*, \bullet)$. Nhóm $(\{1, -1\}, \bullet)$ là nhóm con của nhóm $(\{1, -1, i, -i\}, \bullet)$.

3) Cho $(G, \bullet)$ là một nhóm. Khi đó $Z(G) = \{x \in G : xg = gx, \text{với mọi } g \in G\}$ là một nhóm con giao hoán của nhóm G. Thật vậy, với mọi $a, b \in Z(G)$ và với mọi $g \in G$ ta có

$$(ab)g = a(bg) = a(gb) = (ag)b = (ga)b = g(ab),$$

tức là $ab \in Z(G)$.

Mặt khác, từ $ag = ga$ suy ra
$$a^{-1}(ag)a^{-1} = a^{-1}(ga)a^{-1}$$
$$(a^{-1}a)(ga^{-1}) = (a^{-1}g)(aa^{-1})$$
$$ga^{-1} = a^{-1}g,$$

tức là $a^{-1} \in Z(G)$. Tính giao hoán của (ZG) là rõ ràng. Nhóm con Z(G) được gọi là **tâm của nhóm G**.

4) Cho $(9, +)$ là nhóm nhân các số nguyên. Đặt $n9 = \{nk : k \in 9\}$. Khi đó n9 là một nhóm con của $(9, +)$. Hơn nữa, mọi nhóm con của $(9, +)$ đều có dạng m9 với m là một số nguyên nào đó.
Thật vậy, n9 là nhóm con vì $nx - ny = n(x - y) \in n9$. Bây giờ, gọi H là một nhóm con bất kì của nhóm $(9, +)$. Nếu $H = \{0\}$ thì $H = 09$. Nếu $H \neq \{0\}$ thì tồn tại số nguyên $k \in H$ với $k \neq 0$. Khi đó $-k$ cũng thuộc H do H là nhóm con. Như vậy, trong H có ít nhất một số dương. Gọi m là số dương nhỏ nhất trong H. Ta sẽ chỉ ra $H = m9$. Trước hết $H \subset m9$, thật vậy, lấy x là một phần tử bất kì của H. Từ phép chia trong 9 ta được $x = mq + r$, với $0 \leq r < m$. Nếu $0 < r < m$ thì từ $r = x - mq \in H$ dẫn đến mâu thuẫn với việc m là số dương nhỏ nhất của H, vậy ta phải có $r = 0$. Từ đó $x = mq \in m9$. Bao hàm thức ngược lại $m9 \subset H$ là rõ ràng.

4) Giao của một họ bất kì các nhóm con của một nhóm G cũng là một nhóm con của nhóm G.
Thật vậy, xét một họ bất kì $\{X_i\}_{i \in I}$ các nhóm con của $(G, \bullet)$ và X là giao của chúng. Lấy hai phần tử bất kì x, y của X, khi đó $x, y \in X_i$ với mọi $i \in I$. Vì X_i là các nhóm con nên $xy^{-1} \in X_i$ với mọi $i \in I$, do đó $xy^{-1} \in X$. Từ định lí 3.2 suy ra X là một nhóm con của G.

• NHẬN XÉT: Nếu A là một tập con của nhóm G, thì A sẽ chứa trong ít nhất một nhóm con của G, chẳng hạn G. Theo ví dụ 4) giao của tất cả các nhóm con của G chứa A cũng là một nhóm con chứa A. Có thể kiểm tra dễ dàng rằng đó là nhóm con bé nhất chứa A, tức là nó chứa trong mọi nhóm con chứa A của G.

3.3 Nhóm con sinh bởi một tập con của nhóm

• Có một con đường tổng quát để thu được các nhóm con từ một nhóm. Xét S là một tập con khác ∅ của nhóm (G, •). Đặt:

$$< S > = \{a_1^{\varepsilon_1} a_2^{\varepsilon_2} \dots a_n^{\varepsilon_n} : a_i \in S,\ \varepsilon_i = \pm 1, n \in \angle\}$$

Khi đó, < S > là nhóm con của G và là nhóm con bé nhất chứa S.
Thật vậy, nếu x, y ∈ < S > thì rõ ràng $xy^{-1} \in < S >$, tức là < S > là một nhóm con của G. Gọi H là giao của tất cả các nhóm con của G chứa S. Vì nhóm con H chứa mọi phần tử a ∈ S nên < S > ⊂ H. Vì < S > hiển nhiên chứa S nên < S > = H. Vậy, < S > là nhóm con bé nhất của G chứa S.
• < S > được gọi là **nhóm con sinh bởi S**. Ta cũng nói rằng S tập các **phần tử sinh** của < S >.

• Nếu S = {a} thì < S > gồm tất cả các phần tử có dạng a^n với n ∈ 9 . Trong trường hợp này ta thường viết (a) thay cho < {a}> và gọi nó là **nhóm con cyclic của G sinh bởi a**.

• VÍ DỤ:
1) Xét nhóm cộng các số nguyên (9 , +). Khi đó (1) = 9.

2) Xét nhóm nhân các số phức (∀, •). Khi đó (i) = {1, –1, i, – i }.

4. Nhóm con chuẩn tắc - Nhóm thương

4.1 Lớp kề - Quan hệ tương đương xác định bởi một nhóm con

• Cho (G, •) là một nhóm, H là một nhóm con của nó và a là phần tử của G. Tập hợp tất cả các phần tử ax với x ∈ H được gọi là **lớp kề trái** (hay **lớp ghép trái**) **của H trong G**. Ta kí hiệu nó bởi aH.

• Cho (G, •) là một nhóm, H là một nhóm con của nó. Trên G ta xác định một quan hệ ~ như sau

$$x \sim y \Leftrightarrow x^{-1}y \in H$$

Quan hệ ~ xác định ở trên là một quan hệ tương đương. Thật vậy, vì H là nhóm con nên $x^{-1}x = 1 \in H$, tức là x ~ x (tính phản xạ). Giả sử x và y là hai phần tử bất kì của G sao cho x ~ y, tức là $x^{-1}y \in H$. Vì H là nhóm con nên ta có $(x^{-1}y)^{-1} = y^{-1}x \in H$, tức là y ~ x. Vậy ~ có tính đối xứng. Cuối cùng, giả sử x, y, z là ba phần tử bất kì của G sao cho x ~ y và y ~ z, tức là $x^{-1}y, y^{-1}z \in H$. Từ H là nhóm con suy ra $(x^{-1}y)(y^{-1}z) = x^{-1}(y\,y^{-1})z = x^{-1}z \in H$. Vậy ~ là bắc cầu.

• NHẬN XÉT:

1) Quan hệ tương đương ~ nói đến ở trên chia G thành các lớp tương đương. Kí hiệu $\bar{a}$ sẽ được dùng để chỉ lớp tương đương chứa phần tử a, khi đó

$$\bar{a} = aH = \{ax : x \in H\}$$

Thật vậy, giả sử b là một phần tử bất kì thuộc lớp tương đương $\bar{a}$, khi đó a~b, tức là $a^{-1}b \in H$, từ đó $b = a(a^{-1}b) \in aH$. Vậy $\bar{a} \subset aH$. Ngược lại, giả sử b là một phần tử bất kì thuộc aH, khi đó tồn tại một phần tử x thuộc H sao cho b = ax hay $x = a^{-1}b$, tức là $a^{-1}b \in H$. Vậy a ~ b và từ đó $aH \subset \bar{a}$.

Từ nhận xét 1) suy ra rằng, đối với hai lớp kề bất kì aH và bH của H trong G thì hoặc là chúng trùng nhau hoặc là chúng rời nhau.

2) Lớp kề aH trùng với H khi và chỉ khi $a \in H$. Thật vậy, giả sử có aH = H. Gọi e là phần tử đơn vị của G, do H là nhóm con nên $e \in H$, từ đó $a = ae \in aH = H$. Ngược lại, giả sử $a \in H$, ta sẽ chỉ ra aH = H. Vì H là nhóm con nên từ $a \in H$ suy ra $ax \in H$ với mọi $x \in H$ và điều này có nghĩa là $aH \subset H$. Bây giờ giả sử b là một phần tử bất kì của H. Vì H là nhóm con nên $a^{-1} \in H$ và $a^{-1}b \in H$, từ đó $b = (a\,a^{-1})b = a(a^{-1}b) \in aH$. Vậy $H \subset aH$.

• Hoàn toàn tương tự, ta kí hiệu Ha là **lớp kề phải của H trong G**, nó gồm tất cả các phần tử xa với $x \in H$, và trùng với lớp tương đương $\bar{a}$ chứa phần tử a trong quan hệ tương đương được xác định bởi

$$x \sim y \Leftrightarrow xy^{-1} \in H$$

Trong các phần sau, nếu không chỉ rõ, ta nói lớp kề có nghĩa là lớp kề trái.

• Nếu dùng dấu + để kí hiệu phép toán trong nhóm G, thì lớp kề trái và phải của H trong G sẽ được viết là

$$a + H = \{a + x : x \in H\}; \quad H + a = \{x + a : x \in H\}$$

Còn các quan hệ tương đương sẽ được viết là

$$x \sim y \Leftrightarrow (-x) + y \in H; \quad x \sim y \Leftrightarrow y + (-x) \in H)$$

4.2 Mệnh đề

Cho G là một nhóm, và H là một nhóm con. Khi đó số các phần tử của một lớp kề aH bằng số các phần tử trong H.

Chứng minh: Xét ánh xạ $H \to aH$, $x \mapsto ax$. Ánh xạ này là một song ánh, thật vậy rõ ràng nó là tòan ánh, hơn nữa nó là đơn ánh vì từ $ax = ax'$ suy ra $x = x'$ (luật giản ước trong nhóm). Vì G hữu hạn nên H cũng hữu hạn, từ đó số phần tử của H phải bằng số phần tử của aH. □

• Cho G là một nhóm, và H là một nhóm con. Số các lớp kề rời nhau của H trong G được gọi là **chỉ số của H trong G**. Chỉ số này tất nhiên có thể là vô hạn. Nếu G là nhóm hữu hạn, thì chỉ số của một nhóm con bất kì là hữu hạn. Chỉ số của một nhóm con H trong G sẽ được kí hiệu là (G : H).

4.3 Định lí (Lagrange)

Cho G là một nhóm hữu hạn và H là một nhóm con. Khi đó

$$(\text{cấp của } G) = (G : H) \times (\text{cấp của } H)$$

Chứng minh:
Vì G hữu hạn nên số các lớp kề (G : H) là hữu hạn, khi đó G được phân hoạch thành (G : H) lớp, số phần tử của mỗi lớp, theo mệnh đề 5.3, bằng cấp của H.
Từ đó suy ra đẳng thức cần chứng minh. □

• NHẬN XÉT:
1) Định lí Lagrange cũng chỉ ra rằng cấp của một nhóm con của một nhóm hữu hạn là ước của cấp của nhóm đó.

2) Sau đây là một ứng dụng của định lí Lagrange. Giả sử G là một nhóm hữu hạn cấp n. Khi đó, với mọi $x \in G$ ta có $x^n = e$.

Thật vậy, xét nhóm con cyclic của G sinh bởi x : $H = (x) = \{x^k, k \in 9\}$.Vì H hữu hạn nên tồn tại những lũy thừa cuả x bằng nhau, chẳng hạn $x^k = x^m$ (với $k > m$). Khi đó, $x^{k-m} = x^{m-m} = a^0 = e$. Vậy tồn tại những số mũ nguyên dương l sao cho $x^l = e$. Gọi s là số nguyên dương nhỏ nhất có tính chất ấy. Ta chỉ ra rằng các phần tử $x^0 = e, x, x^2, \ldots, x^{s-1}$ là khác nhau, và mọi phần tử của H đều bằng một trong các phần tử ấy. Trước hết các phần tử nói ở trên là khác nhau, vì nếu $x^k = x^m$ với $0 \le m < k \le s-1$, thì ta có $x^{k-m} = e$ với $0 < k - m < s$, nhưng điều này mâu thuẩn với giả thiết về s. Bây giờ, giả sử a là một phần tử bất kì của H, tức là $a = x^k$ với k là một số nguyên nào đó. Chia k cho s ta được $k = sq + r$ với $0 \le r < s$. Khi đó $a = x^k = x^{sq+r} = (x^s)^q x^r = e x^r = x^r$. Từ đó suy ra cấp của H bằng s. Theo định lí Lagrange thì s là ước của n, tức là $n = sp$.Từ đó $x^n = x^{sp} = (x^s)^p = e^p = e$.

4.4 Nhóm con chuẩn tắc

• Một nhóm con H của một nhóm G được gọi là **nhóm con chuẩn tắc** nếu và chỉ nếu $xH = Hx$ với mọi $x \in G$

• Có thể phát biểu định nghĩa nhóm con chuẩn tắc dưới dạng tương đương:

Một nhóm con H của nhóm G là chuẩn tắc khi và chỉ khi $x^{-1}a\,x \in H$ với mọi $a \in H$ và mọi $x \in G$.

Ta sẽ chỉ ra rằng hai định nghĩa nêu ở trên là tương đương. Thật vậy, giả sử có xH = Hx với mọi $x \in G$. Gọi a là phần tử bất kì của H, khi đó tồn tại $a' \in H$ sao cho xa = a'x, suy ra $a = x^{-1}a'\,x \in H$. Ngược lại, giả sử có $x^{-1}a\,x \in H$ với mọi $a \in H$ và mọi $x \in G$. Với phần tử a bất kì thuộc H, và $x \in G$ ta chỉ cần chỉ ra tồn tại hai phần tử a' và $a'' \in H$ sao cho xa = a''x và ax = xa', vì khi đó suy ra ngay xH = Hx. Có thể thấy hai phần tử a, a'' cần tìm là $a' = x^{-1}a\,x \in H$ và $a'' = (x^{-1})^{-1}ax^{-1} = x\,ax^{-1} \in H$.

• CHÚ Ý: Điều kiện với mọi $x \in X$: xH = Hx không có nghĩa là với bất kì a thuộc H thì phải có xa = ax mà điều kiện này chỉ có nghĩa là với mỗi $a \in H$ sẽ tồn tại $a' \in H$ sao cho xa = a'x.

• VÍ DỤ:
1) Mọi nhóm con của một nhóm giao hoán đều chuẩn tắc. Chẳng hạn n9 là nhóm con chuẩn tắc của nhóm (9 , +).

2) Tâm của nhóm G, $Z(G) = \{x \in G : gx = xg, \text{ với mọi } g \in G\}$, là nhóm con chuẩn tắc của G. Thật vậy, với mọi $x \in G$, với mọi $h \in Z(G)$ ta có
$x^{-1}h\,x = x^{-1}(h\,x) = x^{-1}(x\,h) = (x^{-1}\,x)\,h = h \in Z(G)$.

3) Nếu S và T là các nhóm con chuẩn tắc của nhóm G thì $S \cap T$ cũng là nhóm con chuẩn tắc của G. Thật vậy, với mọi $x \in G$, với mọi $h \in S \cap T$, vì $h \in S$ và $h \in T$ nên $x^{-1}h\,x \in S$ và $x^{-1}h\,x \in T$, từ đó $x^{-1}h\,x \in S \cap T$.

4) Xét nhóm các phép thế $S_3 = \{\text{song ánh } \sigma : \{1, 2, 3\} \to \{1, 2, 3\}\}$ với phép toán hợp các ánh xạ mà các phần tử là (ở đây, kí hiệu $\sigma = (\sigma(1)\ \sigma(2)\ \sigma(3))$):

$$\sigma_1 = (123),\ \sigma_2 = (132),\ \sigma_3 = (213),\ \sigma_4 = (231),\ \sigma_5 = (312),\ \sigma_6 = (321)$$

Khi đó nhóm con $H = \{\sigma_1, \sigma_4, \sigma_5\}$ là chuẩn tắc vì

$\sigma_1 H = H\sigma_1 = H,\ \sigma_2 H = H\sigma_2 = \{\sigma_2, \sigma_3, \sigma_6\};\ \sigma_3 H = H\sigma_3 = \{\sigma_3, \sigma_2, \sigma_6\};$

$\sigma_4 H = H\sigma_4 = H,\ \sigma_5 H = H\sigma_5 = H,\ \sigma_6 H = H\sigma_6 = \{\sigma_6, \sigma_3, \sigma_2\}.$

4.5 Nhóm thương

• Cho (G, •) là nhóm và H là một nhóm con chuẩn tắc của G. Xét tập G/H gồm các

lớp kề trái aH (cũng là kề phải do H là chuẩn tắc), chú ý rằng nó cũng là tập thương đối với quan hệ tương đương đã nói trong 5.1

Ta sẽ xây dựng một cấu trúc nhóm trên tập G/H bằng cách xác định phép tóan nhân trên G/H như sau

$$aH \bullet bH = abH$$

Với mọi a, a', b, b' $\in$ G, nếu (aH, bH) = (a'H, b'H) thì abH = a'b'H (do $(ab)^{-1}$ a' b' = b^{-1} (a^{-1} a') b' = (b^{-1} (a^{-1} a') b)(b^{-1} b') $\in$ H). Vậy $\bullet$ thực sự là một phép tóan trong trên G/H. Nó có tính kết hợp , phần tử đơn vị là 1_GH, phần tử nghịch đảo của aH là a^{-1}H. Khi đó (G/H, $\bullet$) là một nhóm và được gọi là **nhóm thương của G trên H**.

- Nếu G là nhóm cộng thì phép tóan trên tập thương G/H sẽ được viết

$$(a + H) + (b + H) = (a + b) + H$$

và nhóm thương (G/H, +) có phần tử đơn vị là 0 + H, phần tử nghịch đảo của a + H là (–a) + H

- VÍ DỤ: Xét (9 , +) là nhóm cộng các số nguyên, (m 9 ,+) là nhóm con và là chuẩn tắc do (9 ,+) giao hóan.

Tập thương $^{9}/_{m\,9} = \{ \bar{a} = a + m\,9 : 0 \le a \le m-1\}$

cùng với phép tóan (a + m9) + (b + m9) = (a + b) + m9

tạo thành nhóm thương ($^{9}/_{m\,9}$, +), còn được kí hiệu 9_m , và được gọi là **nhóm các số nguyên modulo m** . Phần tử đơn vị là $\bar{0}$ = 0 + m9, phần tử nghịch đảo của $\bar{a}$ là $\overline{-a}$.

- CHÚ Ý: Trên 9_m , xét phép toán nhân $\bar{a}\ \bar{b} = \overline{ab}$. Nếu m là số nguyên tố thì $9_m - \{ \bar{0} \}$ là nhóm giao hoán với phần tử đơn vị là $\bar{1}$ phần tử nghịch đảo của $\bar{a}$ là $\bar{b}$ với ab $\equiv$ 1(mod m)

- Minh họa trong 9_5

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$

•	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{1}$	$\bar{3}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

5. Đồng cấu nhóm

5.1 Định nghĩa

• Cho $(G, *)$ và $(H, \perp)$ là hai nhóm. Ánh xạ $f : G \to H$ được gọi là một **đồng cấu (nhóm)** nếu nó bảo toàn các phép toán của nhóm, tức là

$$f(a * b) = f(a) \perp f(b) \quad \text{với mọi } a, b \in G.$$

• Một đồng cấu f được gọi là **đơn cấu**, **toàn cấu**, **đẳng cấu** nếu ánh xạ f tương ứng là đơn ánh, toàn ánh, song ánh. Nếu G = H thì đồng cấu f được gọi là một **tự đồng cấu của G**. Một tự đồng cấu song ánh được gọi là một **tự đẳng cấu**. Trong trường hợp $f : G \to H$ là một đẳng cấu thì ta cũng nói nhóm G đẳng cấu với nhóm H, và viết $G \cong H$.

• KÍ HIỆU: $\mathrm{Hom}(G, H) = \{\text{đồng cấu } f: G \to H\}$
$\mathrm{End}(G) = \{\text{tự đồng cấu } f : G \to G\}$
$\mathrm{Aut}(G) = \{\text{tự đẳng cấu } f : G \to G\}$

• VÍ DỤ:

1) $(3^*_+, \bullet) \cong (3, +)$ vì có một đẳng cấu $f : (3^*_+, \bullet) \to (3, +)$, $f(x) = \ln x$, ở đây 3^*_+ là tập các số thực dương và • và + là các phép toán nhân và cộng thông thường.

2) Hai nhóm $(\Theta, +)$ và $(\Theta^*_+, \bullet)$ với các phép toán nhân và cộng thông thường trên tập số hữu tỉ không thể đẳng cấu với nhau. Thật vậy, giả sử có một đẳng cấu $f : (\Theta, +) \to (\Theta^*_+, \bullet)$. Xét số $2 \in \Theta^*_+$, vì f song ánh nên tồn tại $a \in \Theta$ sao cho $2 = f(a) = f(\frac{a}{2} + \frac{a}{2}) = f(\frac{a}{2})f(\frac{a}{2}) = [f(\frac{a}{2})]^2$, nhưng điều này dẫn đến mâu thuẫn vì không có số hữu tỉ nào mà bình phương của nó bằng 2.

3) Cho $(G, \bullet)$ là một nhóm và S(G) là nhóm các hoán vị của tập G. Với mỗi a thuộc G, xét ánh xạ $T_a : G \to G$, $T_a(x) = ax$.

Ta thấy rằng, T_a là một song ánh, thật vậy, nó là đơn ánh vì nếu $ax = ay$ thì $x = y$ (luật giản ước trong một nhóm); nó là toàn ánh vì với mọi $x \in G$ ta có $x = T_a(a^{-1}x)$. Từ đó $T_a \in S(G)$. Người ta gọi T_a là **phép tịnh tiến trái bởi a**.

Bây giờ xét ánh xạ $a \mapsto T_a$ từ nhóm $(G, \bullet)$ đến nhóm $(S(G), o)$ các hóan vị của tập hợp G. Có thể chỉ ra nó là một đơn cấu. Thật vậy, nó là đồng cấu vì với mọi $a, b \in G$ ta có $T_{ab}(x) = abx = T_a(T_b(x))$, nó là đơn ánh vì nếu $T_a(x) = T_b(x)$, tức là $ax = bx$, thì do luật giản ước ta có $a = b$.

Tên gọi của ánh xạ T_a được lấy từ hình học Euclide. Đặt $G = 3^2 = 3 \times 3$, ta hình dung G như một mặt phẳng và mỗi phần tử của G là một vector. Khi đó với $A \in 3 \times 3$, ánh xạ $T_A : G \to G, T_A(X) = X + A$ chính là phép tịnh tiến theo vector A thông thường.

4) Cho $(G, +)$ và $(H,+)$ là hai nhóm giao hoán. Ta có thể làm $Hom(G, H)$ trở thành một nhóm như sau. Nếu $f, g \in Hom(G, H)$ ta xác định $f + g : G \to H$ là ánh xạ được cho bởi $(f + g)(x) = f(x) + g(x)$ với mọi $x \in G$. Việc kiểm tra nó là một nhóm là không khó, phần tử đơn vị là đồng cấu $x \mapsto 0$, phần tử nghịch đảo của f là đồng cấu $x \mapsto -f(x)$.

5) Cho H là một nhóm con của nhóm G. Khi đó ánh xạ $i : H \to G, i(x) = x$ là một đơn cấu, gọi là **đơn cấu chính tắc**.

6) Cho H là một nhóm con chuẩn tắc của nhóm G. Khi đó ánh xạ

$$\pi : G \to G/H, \ \pi(x) = xH,$$

là một đồng cấu nhóm từ nhóm G đến nhóm thương G/H. Thật vậy, vì ta có $\pi(xy) = xyH = xH\ yH = \pi(x)\pi(y)$. Hơn nữa, đồng cấu này là một toàn cấu, gọi là **tòan cấu chính tắc**.

5.2 Ảnh và nhân của đồng cấu

• Cho $f : G \to H$ là một đồng cấu từ nhóm $(G, \bullet)$ đến nhóm $(H, \bullet)$, các phần tử đơn vị của G và H được kí hiệu lần lượt là 1_G và 1_H. Ta sẽ gọi các tập hợp $Imf = f(G) = \{f(x), x \in G\}$ và $Kerf = f^{-1}(1_H) = \{x \in G : f(x) = 1_H\}$ lần lượt là **ảnh** và **nhân của đồng cấu f**.

5.3 Các tính chất của đồng cấu nhóm

• *Tính chất 1* Hợp của hai đồng cấu nhóm là một đồng cấu nhóm. Hơn nữa, hợp của hai đẳng cấu là một đẳng cấu.

Chứng minh: Giả sử f : (X. •) → (Y, •) và g : (Y, •) → (Z, •) là hai đồng cấu nhóm. Gọi a, b là hai phần tử bất kì của X. Khi đó go f là một đồng cấu vì

(go f)(ab) = g(f(ab)) = g [f(a)f(b)] = g(f(a))g(f(b)) = (go f)(a) (go f)(b) □

• *Tính chất 2:* Cho f : (G, •) →(H, •) là một đồng cấu nhóm; 1_G ,1_H lần lượt là phần tử đơn vị của G và H. Khi đó

a) $f(1_G) = 1_H$.

b) $f(a^{-1}) = [f(a)]^{-1}$ với mọi a ∈ G.

Chứng minh:

a) Ta có $f(1_G)1_H = f(1_G) = f(1_G1_G) = f(1_G)f(1_G)$, từ đó $f(1_G) = 1_H$ (luật giản ước)

b) Suy ra từ $f(a)f(a^{-1}) = f(aa^{-1}) = f(1_G) = 1_H$. □

• *Tính chất 3:* Giả sử f : (G, •) → (H, •) là một đồng cấu nhóm. Khi đó

a) Nếu A là một nhóm con của G thì f(A) là một nhóm con của H. Hơn nữa nếu A chuẩn tắc thì f (A) cũng chuẩn tắc.

b) Nếu B là một nhóm con của H thì $f^{-1}(B)$ là một nhóm con của G. Hơn nữa nếu B chuẩn tắc thì $f^{-1}(B)$ cũng chuẩn tắc.

Chứng minh:

a) Vì A là nhóm con nên 1_G ∈A, do đó $f(1_G) = 1_H \in f(A)$, tức là f(A) ≠ ∅.
Giả sử y_1, y_2 là hai phần tử bất kì của f(A). Khi đó, tồn tại $x_1, x_2 \in A$ sao cho $y_1 = f(x_1)$, $y_2 = f(x_2)$. Ta có $y_1y_2^{-1} = f(x_1)\,[f(x_2)]^{-1} = f(x_1)\,f(x_2^{-1}) = f(x_1x_2^{-1})$. Mặt khác, vì A là nhóm con của G nên $x_1x_2^{-1} \in A$, do đó $y_1y_2^{-1} = f(x_1x_2^{-1}) \in f(A)$. Vậy f(A) là nhóm con.

b) Vì B là nhóm con nên $1_H \in B$, do đó $f(1_G) = 1_H \in B$, suy ra $1_G \in f^{-1}(B)$, tức là $f^{-1}(B) \neq \emptyset$. Giả sử x_1, x_2 là hai phần tử bất kì của $f^{-1}(B)$. Khi đó $f(x_1), f(x_2) \in B$. Ta có $f(x_1x_2^{-1}) = f(x_1)\,f(x_2^{-1}) = f(x_1)\,[f(x_2)]^{-1}$. Mặt khác, vì B là nhóm con của H nên $f(x_1)\,[f(x_2)]^{-1} = f(x_1x_2^{-1}) \in B$. Từ đó $x_1x_2^{-1} \in f^{-1}(B)$.
Giả sử B là chuẩn tắc. Với mọi $a \in f^{-1}(B)$ và $x \in G$, do f là đồng cấu nên ta có $f(x^{-1}ax) = f(x^{-1})f(a)f(x) = [f(x)]^{-1}f(a)f(x)$. Vì $f(a) \in B$ và B chuẩn tắc nên $[f(x)]^{-1}f(a)f(x)$ thuộc B. Từ đó suy ra $x^{-1}ax$ thuộc $f^{-1}(B)$, tức là $f^{-1}(B)$ là chuẩn tắc. □

• NHẬN XÉT: Từ tính chất 3 suy ra ngay rằng, Ker f = $f^{-1}(1_H)$ và Im f = f(G) lần lượt là các nhóm con của G và H, hơn nữa Ker f là nhóm con chuẩn tắc.

• *Tính chất 4:* Giả sử f : (G, •) → (H, •) là một đồng cấu nhóm. Khi đó

a) f là đơn cấu khi và chỉ khi Kerf = $\{1_G\}$.

b) f là toàn cấu khi và chỉ khi Imf = H

Chứng minh:

a) • Giả sử f là đơn cấu. Trước hết ta có $\{1_G\} \subset$ Kerf vì $f(1_G) = 1_H$. Với x bất

kì thuộc Kerf, ta có $f(x) = 1_H = f(1_G)$, do f đơn ánh nên suy ra $x = 1_G$, từ đó Kerf $\subset \{1_G\}$.

- Bây giờ giả thiết Kerf $= \{1_G\}$ và giả sử $f(x_1) = f(x_2)$ với mọi $x_1, x_2 \in G$. Khi đó ta có $f(x_1)[f(x_2)]^{-1} = 1_H$, suy ra $f(x_1 x_2^{-1}) = 1_H$, từ đó $x_1 x_2^{-1} \in$ Kerf $= \{1_G\}$, tức là $x_1 x_2^{-1} = 1_G$ hay $x_1 = x_2$. Vậy f là đơn ánh.

b) Suy ra trực tiếp từ định nghĩa của toàn ánh. □

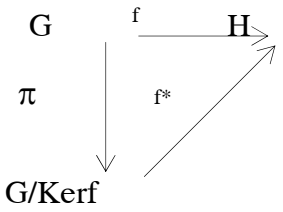
- *Tính chất 5:* Giả sử $f : (G, \bullet) \to (H, \bullet)$ là một đồng cấu nhóm. Khi đó

$$f(a^n) = [f(a)]^n \text{ với mọi } n \in 9$$

Chứng minh: Qui nạp cho $n \in \angle$, còn lại sử dụng định nghĩa lũy thừa âm. □

5.4 Định lí (cơ bản của đồng cấu nhóm)

Cho f là một đồng cấu từ nhóm G đến nhóm H và $\pi : G \to G/\text{Kerf}$ là toàn cấu chính tắc từ nhóm G đến nhóm thương G/kerf . Khi đó tồn tại duy nhất một đồng cấu $f^* : G/\text{kerf} \to H$ sao cho $f = f^* o\ \pi$, tức là biểu đồ sau giao hoán:



Hơn nữa, f^* là một đơn cấu và $\text{Im } f^* = f(G) = \text{Im} f$

Chứng minh: Đặt K = Kerf và sẽ chỉ ra đồng cấu cần tìm là

$$f^* : G/K \to H,\ f^*(xK) = f(x)$$

- Trước hết f^* là được xác định đúng đắn, thật vậy giả sử $xA = yA$ thì ta có $x^{-1}y \in A = \text{Kerf}$, từ đó $f(x^{-1}y) = f(x^{-1})f(y) = [f(x)]^{-1}f(y) = 1_H$, hay $f(x) = f(y)$.

- f^* là một đồng cấu vì $f^*(xA.yA) = f^*(xyA) = f(xy) = f(x)f(y) = f^*(xA)f^*(yA)$

- f^* là duy nhất, thật vậy giả sử có một đồng cấu khác $g^* : G/A \to H$ sao cho $f = g^* o\ \pi$. Khi đó với mọi $xA \in G/A$ ta có

$$g^*(xA) = g^*(\pi(x)) = (g^* o\ \pi)(x) = f(x) = (f^* o\ \pi)(x) = f^*(\pi(x)) = f^*(xA)$$

tức là $g^* = f^*$.

- f^* là đơn ánh, thật vậy giả sử có $f^*(xA) = f^*(yA)$, suy ra $f(x) = f(y)$, từ đó $f(x^{-1}y) = f(x^{-1})f(y) = [f(x)]^{-1}f(y) = 1_H$, tức là $x^{-1}y \in \text{Kerf} = A$, vậy $xA = yA$.

• Vì π là toàn cấu nên $f(G) = (f^* o \pi)(G) = f^*(\pi(G)) = f^*(G/K) = \text{Im } f^*$ □

5.5 Hệ quả

1) Với mọi đồng cấu nhóm $f : G \to H$ ta có $f(G) \cong G/\text{Ker}f$
2) Với mọi toàn cấu nhóm $f : G \to H$ ta có $H \cong G/\text{Ker}f$

• VÍ DỤ:

Với $m \in \angle$, xét đồng cấu $f : (9, +) \to (\forall^*, \bullet)$, $f(k) = \cos \frac{2k\pi}{m} + i\sin \frac{2k\pi}{m}$, khi đó ta có

$\text{Im}f = f(9) = \{ \cos \frac{2k\pi}{m} + i\sin \frac{2k\pi}{m}, k = 0, 1, 2,\ldots, m-1\} = \sqrt[m]{1}$

$\text{Ker}f = \{k \in 9 : \cos \frac{2k\pi}{m} + i\sin \frac{2k\pi}{m} = 1\} = \{km, m \in 9\} = m9$

Theo hệ quả 5.5 thì $f(9) \cong 9_m = {}^9/_{m9}$

6. Nhóm cyclic

6.1 Định nghĩa

• Một nhóm G được gọi là **cyclic**, nếu và chỉ nếu tồn tại một phần tử $a \in G$ sao cho $G = (a) = \{a^n, n \in 9\}$, khi đó a gọi là **phần tử sinh của G**.

Nếu nhóm cyclic G được viết theo lối cộng thì mọi phần tử $x \in G$ đều có dạng $x = na$, $n \in 9$.

• VÍ DỤ:

1) Nhóm $(9, +)$ là nhóm cyclic với phần tử sinh là 1 hay –1. Đó cũng là phần tử sinh duy nhất của 9, vì giả sử có $a \neq \pm 1$ là một phần tử sinh thì do $na \neq 1$ với mọi $n \in 9$ nên $1 \notin 9$.

2) Nhóm $(9_m, +)$ là nhóm cyclic với phần tử sinh là $\bar{1}$. Chú ý rằng nhóm này là hữu hạn cấp m.

6.2 Cấp của một phần tử trong nhóm

• Cho $(G, \bullet)$ là một nhóm. Một phần tử $a \in G$ được gọi là có **cấp hữu hạn** nếu tồn tại một số nguyên $k > 0$ sao cho $a^k = 1_G$. Trong trường hợp này ta gọi số nguyên dương nhỏ nhất m sao cho $a^m = 1_G$ là **cấp của phần tử a**, và kí hiệu $m = \text{ord}(a)$

• Phần tử $a \in G$ được gọi là **có cấp vô hạn** nếu và chỉ nếu với mọi số nguyên $k \neq 0$ ta có $a^k \neq 1_G$.

6.3 Định lí (phân loại nhóm tuần hoàn)

Giả sử G = (a) là nhóm cyclic với phần tử sinh là a. Khi đó

a) Nếu a có cấp n thì $G \cong (9_n, +)$
b) Nếu a có cấp vô hạn thì $G \cong (9, +)$

Chứng minh: Xét toàn cấu $f : (9, +) \to G, f(k) = a^k$.

a) Nếu a có cấp n thì Kerf = n9, và theo hệ quả 5.5 của định lí đồng cấu ta có $G \cong 9_n = {}^{9}/_{n9}$.

b) Nếu a có cấp vô hạn thì rõ ràng Kerf = {0}, và cũng theo hệ quả 5.5 của định lí đồng cấu ta có $G \cong {}^{9}/_{\{0\}} \cong (9, +)$. □

NHẬN XÉT: Từ định lí 6.3 suy ra mọi nhóm cyclic G mà phần tử sinh của nó có cấp n thì G là nhóm hữu hạn cấp n, cụ thể $G = \{a^0 = e, a, a^2, \ldots, a^{n-1}\}$; còn nếu phần tử sinh có cấp vô hạn thì G là nhóm vô hạn.

7. Tác động của một nhóm lên một tập hợp

7.1 Định nghĩa:

• Cho một tập hợp X và một nhóm G. Nói rằng nhóm G tác động lên tập hợp X nếu và chỉ nếu tồn tại một ánh xạ $G \times X \to X, (g, x) \mapsto g.x$ sao cho
a) $e.x = x$ với mọi $x \in X$, và e là phần tử đơn vị của G
b) $(g.h).x = g.(h.x)$, với mọi $g, h \in G$, với mọi $x \in X$.

• VÍ DỤ:
1) Có thể cho nhóm G tác động lên chính nó theo các cách sau

a) **Phép tịnh tiến trái** $G \times G \to G, (g, x) \mapsto g.x$
b) **Phép tịnh tiến phải** $G \times G \to G, (g, x) \mapsto xg^{-1}$
c) **Phép liên hợp** $G \times G \to G, (g, x) \mapsto gxg^{-1}$

Ta chỉ ra, chẳng hạn phép liên hợp là một tác động nhóm, thật vậy rõ ràng ta có $e.x = exe^{-1} = x$ và $(g.h).x = (gh)x(gh)^{-1} = g(hxh^{-1})g^{-1} = g(h.x)g^{-1} = g.(h.x)$.

2) Nhóm G có thể tác động liên hợp lên tập các tập con P(G) của nó theo cách sau: $G \times P(G) \to P(G), (g, A) \mapsto gAg^{-1} = \{ gag^{-1}, a \in A\}$.

7.2 Nhóm con ổn định của một phần tử

• Cho nhóm G tác động trên tập X và $x \in X$. Khi đó, tập hợp

$$G_x = \{g \in G : g.x = x\}$$

là một nhóm con của G, thật vậy vì $e \in G_x$ nên $G_x \neq \emptyset$. Mặt khác, với mọi $g, h \in G_x$ ta có $x = g.x = g.(h^{-1}.h.x) = (g.h^{-1})(h.x) = (g.h^{-1})x$, tức là $h.g^{-1} \in G_x$.
Ta sẽ gọi G_x là **nhóm con ổn định của phần tử** $x \in G$

• VÍ DỤ:
1) Nếu nhóm G tác động lên chính nó bằng liên hợp thì

$$G_x = \{g \in G : g.xg^{-1} = x\} = \{g \in G : g.x = x.g\}.$$

Tập hợp này được gọi là **cái tâm hóa của x**.

2) Nếu nhóm G tác động lên tập P(G) các tập con của nó nó bằng liên hợp thì

$$G_A = \{g \in G : g.Ag^{-1} = A\} = \{g \in G : g.A = A.g\}.$$

Tập hợp này được gọi là **cái chuẩn hóa của A**.

7.3 Quỹ đạo của một phần tử

• Cho nhóm G tác động trên tập X và $x \in X$, khi đó tập $G.x = \{g.x, g \in G\}$ được gọi là **qũi đạo của phần tử x đối với nhóm G**.

• NHẬN XÉT: Hai qũi đạo của hai phần tử x, y của X hoặc rời nhau hoặc trùng nhau. Thật vậy, nếu $s \in G_x \cap G_y$ thì $s = gx = g'y$ với g, g' là hai phần tử nào đó của G. Do đo $G.s = G.g.x = G.g'.y$. Vậy, $G_x = G_y = G_s$.

Như vậy tập X là hợp của các qũi đạo rời nhau $X = \bigcup_{i \in I} G.x_i$, trong đó x_i là các phần tử của các qũi đạo khác nhau, và I là một tập chỉ số.

8. Nhóm đối xứng

8.1 Định nghĩa

• Nếu X là tập khác rỗng, S(X) là tập các song ánh từ X lên X thì đối với phép hợp các ánh xạ, S(X) là một nhóm mà ta thường gọi là nhóm đối xứng (hoặc còn gọi là nhóm hoán vị) trên X. Một tính chất lý thú của nhóm đối xứng là kết quả sau đây

8.2 Định lí (Ceyley)

Mọi nhóm (G, •) đều là nhóm con của nhóm đối xứng S(G).

Chứng minh:
Xét đơn cấu $f : G \to S(G)$, $f(a) = f_a$ với $f_a(x) = ax \quad \forall x \in G$ □

8.3 Nhóm đối xứng S_n

• Nếu $X = \{1,2,...,n\}$, $n \geq 2$, thì nhóm S(X) được gọi là nhóm đối xứng bậc n và kí hiệu là S_n . Mỗi phần tử $\sigma \in S_n$ được gọi là một phép thế, hay hóan vị của {1,2,...,n}, thường được viết dưới dạng :

$$\sigma = \begin{pmatrix} 1 & 2 & ... & n \\ \sigma(1) & \sigma(2) & ... & \sigma(n) \end{pmatrix} \quad \text{hay đơn giản hơn } \sigma = (\sigma(1)\ \sigma(2)\ .\ .\ .\sigma(n)).$$

8.4 r - chu trình

• Một hóan vị $\sigma \in S_n$ gọi là **r-chu trình** nếu có một tập con $\{j_1,..., j_r\}$ gồm r phần tử của {1,2,...,n} sao cho

$$\begin{cases} \sigma(j_i) = j_{i+1}, \forall j = 1,2,..., r-1, \sigma(j_r) = j_1 \\ \sigma(m) = m \qquad , \forall m \neq j_1, j_2,..., j_r \end{cases}$$

• Tập hợp $\{j_1,..., j_r\}$ được gọi là **giá của r - chu trình** σ**,** và thường kí hiệu là $\sigma = (j_1,..., j_r)$ hay $j_1 \to j_2 \to ... \to j_r \to j_1$.

• VÍ DỤ: $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 2 & 4 & 3 \end{pmatrix}$ là 3 - chu trình (2,5,3)

• Một 2-chu trình được gọi là **chuyển vị**.

• Hai chu trình $(j_1,..., j_r)$ và $(h_1,..., h_s)$ được gọi là rời nhau nếu và chỉ nếu

$$\{j_1,..., j_r\} \cap \{h_1,..., h_s\} = \varnothing$$

• NHẬN XÉT*:*

1) Ta xem $\sigma = id$ là 1-chu trình, id = (i), và thường viết id = (1).
2) Nếu σ là một chuyển vị thì $\sigma = \sigma^{-1}$.
3) Tích các chu trình rời nhau có tính chất giao hoán.
4) Trong r-chu trình $\sigma = (j_1,..., j_r)$ ta có $j_{k+1} = \sigma^k(j_1)$, k = 1, 2, ..., r –1.

8.5 Tính chất

1) $(j_1, j_2, .., j_r) = (j_2, j_3, .., j_r, j_1) = \ldots = (j_r, j_1, .., j_{r-2}, j_{r-1})$

2) $(j_1, j_2, .., j_r)^m = \begin{pmatrix} j_1 & j_2 & \cdots & j_r \\ j_{m+1} & j_{m+2} & \cdots & j_{m+r} \end{pmatrix}$,

ở hàng dưới $j_{r+h} = j_k$ nếu $h \equiv k(\mod r)$

3) ord $(j_1, j_2, .., j_r) = r$.

Chứng minh: 1) suy ra từ định nghĩa, 2) chứng minh bằng qui nạp và 3) suy ra trực tiếp từ 2) □

8.6 Định lí

Mọi $\sigma \in S_n$ luôn có thể phân thành tích một số hữu hạn các chuyển vị.

Chứng minh : Ta chứng minh bằng quy nạp theo n
Với n = 2 là hiển nhiên, giả sử định lí đúng với n –1. Xét $\sigma \in S_n$ và giả sử $\sigma(n) = k$. Gọi ρ là chuyển vị (k, n). Suy ra : $(\rho\sigma)(n) = n$, tức là $\rho\sigma$ xem như là phần tử của S_{n-1}. Theo giả thiết quy nạp $\rho\sigma$ là tích của những chuyển vị $\rho\sigma = \sigma_1 \ldots \sigma_k$. Vì $\rho = \rho^{-1}$ nên : $\sigma = \rho\sigma_1 \ldots \sigma_k$. □

8.7 Định lí

Mọi phần tử của S_n đều có thể phân tích thành tích các chu trình đôi một rời nhau, sự phân tích trên là duy nhất (sai khác về thứ tự các chu trình).

Chứng minh :

1) *Sự tồn tại* Ta bắt đầu với dãy $1, \sigma(1), \sigma^2(1), \ldots, \sigma^k(1), \ldots$ (1)
Vì n + 1 số tự nhiên $1, \sigma(1), \sigma^2(1), \ldots, \sigma^n(1)$ đều thuộc {1, 2, …, n} nên tồn tại s, t $\in$ {0,1, 2, …, n} sao cho s < t và $\sigma^s(1) = \sigma^t(1)$. Nếu đặt m = t – s $\in$ {1, 2, …, n} thì ta có $\sigma^m(1) = 1$. Vậy tập hợp {q $\in$ {1, 2, …, n} : $\sigma^q(1) = 1$} là khác rỗng và do đó có số bé nhất p. Khi đó p số tự nhiên $1, \sigma(1), \ldots, \sigma^{p-1}(1)$ là khác nhau từng đôi một, vì nếu tồn tại s, t $\in$ {0,1, 2, …, p –1} sao cho s < t và $\sigma^s(1) = \sigma^t(1)$ thì sẽ có $\sigma^m(1) = 1$ với m = t – s $\in$ {1, 2, …, p –1}, trái với tính chất của p. Như vậy từ dãy (1) ta tìm được một p - chu trình

$$1 \to \sigma(1) \to \sigma^2(1) \to \ldots \to \sigma^{p-1}(1) \to 1$$

. Nếu $2 \notin (1, \sigma(1), \sigma^2(1), \ldots, \sigma^{p-1}(1))$ thì xét dãy $2, \sigma(2), \sigma^2(2), \ldots, \sigma^k(2), \ldots$ và

lập luận tương tự như trên, từ dãy này tìm được một q - chu trình

$$2 \to \sigma(2) \to \sigma^2(2) \to \ldots \to \sigma^{q-1}(2) \to 1$$

. Bằng cách này, sau một số hữu hạn bước, ta tìm được các chu trình rời nhau mà hợp của chúng là σ.

2)*Sự duy nhất.* Giả sử $\sigma = c_1 \text{ o } c_2 \text{ o } \ldots \text{ o } c_r = d_1 \text{ o } d_2 \text{ o } \ldots \text{ o } d_s$ là hai dạng phân tích của σ thành các chu trình từng đôi một rời nhau. Nếu $\sigma = id$ thì khẳng định là rõ ràng. Giả sử $\sigma \neq id$, khi đó tồn tại $i \in \{1, 2, \ldots, n\}$ sao cho $\sigma(i) \neq i$ và $m \in \{1, 2, \ldots, r\}$, $k \in \{1, 2, \ldots, s\}$ sao cho i thuộc giá của chu trình c_m và giá của chu trình d_k. Do ta có thể hoán vị vòng quanh các phần tử trong một chu trình mà không làm nó thay đổi và cũng như trong 1) tồn tại số tự nhiên p sao cho $c_m = d_k = (i, \sigma(i), \ldots, \sigma^{p-1}(i))$. Lặp lại lí luận tương tự cho các chu trình còn lại, ta suy ra r = s và $\{c_1, c_2, \ldots, c_r\} = \{d_1, d_2, \ldots, d_s\}$ □

.VÍ DỤ: Xét $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 7 & 4 & 8 & 5 & 1 & 6 \end{pmatrix} = (1,2,3,7)o(5,8,6)$

Ta bắt đầu ở 1 và tìm được chu trình đầu tiên $1 \to 2 \to 3 \to 7 \to 1$, sau đó bắt đầu với số nhỏ nhất còn lại , trong trường hợp này là 5, vì 4 không thay đổi, $5 \to 8 \to 6 \to 5$.

• Cho $\sigma \in S_n$. Ta nói rằng cặp $(\sigma(i), \sigma(j))$ là một **nghịch thế** trong hoán vị σ (hoặc là một nghịch thế của σ) nếu có $i < j$ và $\sigma(i) > \sigma(j)$. Ta kí hiệu số các nghịch thế của σ là $I(\sigma)$, và gọi $\varepsilon(\sigma) = (-1)^{I(\sigma)}$ là **kí số** của σ. Ta nói rằng hoán vị σ là chẵn(tương ứng: lẻ) nếu $\varepsilon(\sigma) = 1$(tương ứng: $\varepsilon(\sigma) = -1$).

8.8 Hệ quả

Giả sử $\sigma \in S_n$ và $t_1, t_2, \ldots, t_N$ là những chuyển vị của $\{1, 2, \ldots, n\}$
sao cho $\sigma = t_1 \text{ o } t_2 \text{ o } \ldots \text{ o } t_N$. Khi đó, $\varepsilon(\sigma) = (-1)^N$. Như thế một hoán vị chẵn (tương ứng: lẻ) chỉ có thể phân tích thành một số chẵn (tương ứng: lẻ) những chuyển vị.

Chứng minh: Do 8.7, giả sử được rằng σ phân tích một cách duy nhất thành tích những chu trình đôi một không giao nhau như sau

$$\sigma = (i_1\, i_2 \ldots i_r)(j_1\, j_2 \ldots j_s) \ldots (m_1\, m_2 \ldots m_k). \quad (1)$$

Xét ánh xạ $\varphi : S_n \to 9$, $\varphi(\sigma) = (r - 1) + (s - 1) + \ldots + (k - 1)$.

Hiển nhiên là $\varphi(1) = \varphi(id) = 0$. Ta chứng minh rằng tính chất chẵn, lẻ của $\varphi(\sigma)$

cũng là tính chất chẵn, lẻ của số những chuyển vị trong mọi cách phân tích σ thành tích những chuyển vị.

Ta có nhận xét rằng, nếu $\{a, c_1, c_2 \ldots c_h\} \cap \{b, d_1, \ldots d_k\} = \varnothing$ thì

$$(a\, c_1\, c_2 \ldots c_h\, b\, d_1 \ldots d_k)(ab) = (a\, d_1 \ldots d_k)(b\, c_1\, c_2 \ldots c_h)$$

và $$(a\, c_1 c_2 \ldots c_h)(b\, d_1 \ldots d_k)(ab) = (a d_1 \ldots d_k b\, c_1 c_2 \ldots c_h)\ ,$$

Từ đó suy ra $$\varphi(\sigma \circ (ab)) = \varphi(\sigma) \pm 1 \qquad (2)$$

trong đó dấu + hay – phụ thuộc vào việc a, b ở trong hai chu trình khác nhau, hay ở trong cùng một chu trình của (1).

Bây giờ, giả sử σ là tích của m chuyển vị sau đây : $\sigma = (ab)(cd)\ldots(pq)$ (khi đó $\varphi(\sigma)$ là số các chuyển vị trong phân tích).Vì $(ab)^{-1} = (ab)$ nên

$$\sigma \circ (pq) \ldots (cd)(ab) = 1. \qquad (3)$$

Từ (2) và (3) suy ra : $$\varphi(\sigma) \underbrace{\pm 1 \pm 1 \pm \ldots \pm 1}_{m} = 0$$

Như vậy, tính chẵn, lẻ của $\varphi(\sigma)$ là tính chẵn, lẻ của m □

• VÍ DỤ: Đặt $A_n = \{\sigma \in S_n : \varepsilon(\sigma) = 1\}$, khi đó A_n là một nhóm con chuẩn tắc của S_n và cấp của A_n bằng nửa cấp của S_n.
Thật vậy, xét ánh xạ $\varepsilon : (S_n, o) \to (\{-1, 1\}. \bullet), \sigma \mapsto \varepsilon(\sigma)$. Khi đó ε là một toàn cấu nhóm và $\mathrm{Ker}\,\varepsilon = A_n$. Vậy A_n là một nhóm con chuẩn tắc của S_n và do $S_n/A_n \cong \{-1, 1\}$ nên $(S_n : A_n) = 2$. Từ đó theo định lí Lagrange, cấp của A_n bằng nửa cấp của S_n. Nhóm A_n còn được gọi là **nhóm luân phiên.**

BÀI TẬP

1. Cho G = { a,b} và các phép toán trong trên G được xác định bởi

+	a	b
a	a	b
b	b	a

·	a	b
a	b	a
b	a	b

a) Chứng minh rằng (G,+),(G,.) là các nhóm giao hoán.
b) Ánh xạ đồng nhất id : (G,+)→ (G, .) có phải là đẳng cấu nhóm?

2. Cho G = { 1,2,3,4 } và phép toán trong $*$ trên G được xác định bởi

*	1	2	3	4
1	1	2	3	4
2	2	1	4	3
3	3	4	1	2
4	4	3	2	1

Chứng minh rằng (G,$*$) là nhóm giao hoán.

3. Cho G = {1, 2, 3} và $*$ là một phép tóan trong trên G. Biết rằng cấu trúc đại số (G, $*$) là một nhóm. Hãy xác định phép tóan $*$.

4. Cho 9 là tập các số nguyên và trên nó xác định phép toán trong $*$ như sau :

$$m * n = m + n - 1 \quad \text{với } m, n \in 9 .$$

a) Chứng minh rằng (9 ,+) là nhóm giao hoán.
b) Ánh xạ đồng nhất id : (9,+) → (9,$*$) có phải là đẳng cấu nhóm ?

5. Cho G = $3^* \times 3$ và $*$ phép toán trong trên G xác định bởi

$$(x, y) * (x', y') = (xx', xy' + y)$$

a) Chứng minh rằng (G ,$*$) là nhóm không giao hoán.
b) Chứng minh rằng $3^*_+ \times 3$ là một nhóm con của G. (3^*_+ là tập các số thực dương)

6. Cho G = $3^* \times 3$ và $*$ phép toán trong trên G xác định bởi

$$(x, y) * (x', y') = (xx', xy' + \frac{y}{x'})$$

a) Chứng minh rằng (G ,$*$) là nhóm.
b) Hãy xác định tâm Z(G) = {a ∈ G : ag = ga với mọi g ∈ G} của G.
c) Chứng minh rằng $3^*\times\{0\}$, $\{1\}\times 3$, $\Theta^*\times\Theta$ là các nhóm con của G.
d) Chứng minh rằng với k ∈3, tập hợp $H_k = \{(x, k(x - x^{-1})), x \in 3^*\}$ là một nhóm con giao hoán của G.

7. Cho (G,.) là nhóm sao cho mọi x∈ G đều có $x^2 = 1$. Chứng minh rằng G là nhóm giao hoán.

8. Giả sử (G,.) là nhóm có tính chất là tồn tại ba số nguyên dương liên tiếp i sao cho $(ab)^i = a^i b^i$. Chứng minh rằng G là nhóm giao hoán.

9. Cho $E = \{a + b\sqrt{3} : a,b \in Q\}$. Chứng minh rằng
a) (E,+) là nhóm con của (R,+).
b) $(E^*, \bullet)$ là nhóm con của $(R^*, \bullet)$, ở đây $E^* = E - \{0\}$

10. Cho (G, •) là một nhóm, x ∈ G và C(x) = {g ∈ G : gx = xg }. Chứng minh rằng C(x) là nhóm con của G.

11. Cho (G, •) là một nhóm, x ∈ G. Chứng tỏ tập $xGx^{-1} = \{xgx^{-1}, g \in G\}$ là nhóm con của G.

12. Cho G là một nhóm con của nhóm (∀, +) thỏa mãn : $x + ix^2 \in G$ với mọi x ∈[0,1]. Chứng minh rằng G = ∀.

13. Cho một nhóm G hữu hạn cấp 4 sinh bởi S ={x, y} sao cho $x^2 = y^2 = e$ và xy = yx. Hãy xác định tất cả các nhóm con của G. Chỉ ra rằng G = {e, x, y, xy}

14. Cho một nhóm G cấp 8 sinh bởi các phần tử x, y sao cho $x^4 = y^2 = e$ và $xy = yx^3$. Chỉ ra rằng các phần tử x^iy^j ,với i = 0, 1, 2, 3 và j = 0,1 là các phần tử phân biệt của G và từ đó chúng là tất cả các phần tử của G. Xác định tất cả các nhóm con của G.

15. Cho một nhóm G cấp 8 sinh bởi các phần tử i, j, k sao cho

$$ij = k, \quad jk = i, \quad ki = j, \quad i^2 = j^2 = k^2.$$

Kí hiệu i^2 bởi m. Chỉ ra rằng e, i, j, k, m, mi, mj, mk là các phần tử phân biệt của G. Xác định tất cả các nhóm con của G. (Nhóm G như thế được gọi là nhóm quaternion, người ta viết – 1, – i, –j, – k thay cho m, mi, mj, mk)

16. Cho một nhóm G cấp 12 sinh bởi các phần tử x, y sao cho $x^6 = y^2 = e$ và $xy = yx^5$. Chỉ ra rằng các phần tử x^iy^j , với i = 0, 1, 2, 3, 4, 5 và j = 0,1, là các phần tử phân biệt của G. Xác định tất cả các nhóm con của G.

17. Cho (G, •) là một nhóm.
a) Chứng minh rằng (Aut(G), o) là nhóm.(o là phép tóan hợp các ánh xạ)
b)Với $a \in G$, xét ánh xạ $f_a : G \to G$, $f_a(g) = aga^{-1}$, $g \in G$. Chứng minh rằng $f_a \in Aut(G)$.
c) Chứng minh rằng $Int(G) = \{f_a : a \in G\}$ là nhóm con của Aut(G).
d) Chứng minh rằng một nhóm con H của G là chuẩn tắc nếu và chỉ nếu $f_a(H) = H$ với mọi $f_a \in Int(G)$.
e) Chứng minh rằng ánh xạ $\varphi : G \to Int(G)$, $a \mapsto f_a$ là một đồng cấu và $Ker\varphi$ = Z(G) = tâm của G (xem bài 6.b)
f) Chứng minh rằng ánh $G/Z(G) \cong Int(G)$.

18. Cho $f : (9,+) \to (\{-1, 1\},\bullet)$, $f(n) = (-1)^n$. Chứng minh rằng f là toàn cấu nhóm. Hãy xác định Kerf và $9/_{Kerf}$.

19. $V = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} : a,b,d \in 3 \text{ và } ad \neq 0 \right\}$

a) Chứng minh rằng (V, .) là nhóm con của $(GL_3(2), \bullet)$

b) Chứng minh rằng $f : (V,\bullet) \to (3^*, \bullet)$, $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \mapsto a$, là toàn cấu nhóm.

20. Cho (G, •) là một nhóm và a là một phần tử của G. Chứng tỏ rằng:
a) $f : (9, +) \to (G, \bullet)$, $f(n) = a^n$, là một đồng cấu nhóm.
b) Mọi đồng cấu $f: (9, +) \to (G, \bullet)$ thỏa $f(1) = a$ đều có dạng $f(n) = a^n$.
c) Hãy xác định tập End(9,+) = {tự đồng cấu $f : (9, +) \to (9 ,+)$}

21. Cho (G, •) là một nhóm sao cho $f : G \to G$, $f(x) = x^3$, là một toàn cấu nhóm. Chứng tỏ rằng G là nhóm giao hóan.

22. Cho (G, •) là một nhóm sao cho tồn tại số tự nhiên n thỏa mãn tính chất $f_n : G \to G$, $f_n(x) = x^n$, là một toàn cấu nhóm. Chứng tỏ rằng

$$x^{n-1}y = yx^{n-1}, \text{ với mọi } x, y \in G$$

23. Cho (G,+) là nhóm giao hoán. Gọi End(G) tập các tự đồng cấu của G. Trên End(G) xác định phép toán cộng như sau : $(f + g)(x) = f(x) + g(x)$
a) Chứng minh rằng (End(G),+) là nhóm giao hoán.
b) Chứng minh rằng End(9,+) đẳng cấu với (9,+).

24.

a) Chứng minh rằng tập con $A = \{2^n 3^m , m, n \in 9\}$ là nhóm con của nhóm $(\Theta, \bullet)$.
b) Chứng minh rằng A đẳng cấu với nhóm con $B = \{a + bi, a, b \in 9\}$ của nhóm $(\forall, +)$.

25. Chứng minh rằng mọi nhóm con của một nhóm cyclic là nhóm cyclic.

26. Chứng tỏ rằng ảnh đồng cấu của một nhóm cyclic là một nhóm cyclic

27. Cho $(G,\bullet)$ là nhóm cyclic cấp n và $m \in \angle$ là một ước của n. Chứng minh rằng G có đúng một nhóm con cấp m.

28. Chứng minh rằng mọi nhóm cyclic vô hạn có đúng 2 phần tử sinh. Tìm tất cả các phần tử sinh của nhóm tuần hoàn cấp n.

29. Tìm tất cả các tự đồng cấu nhóm của nhóm cyclic cấp n .

30. Cho $(G, \bullet)$ là nhóm; a, b là hai phần tử của G và $f \in End(G)$. Chứng minh rằng

a) $ord(ab) = ord(ba)$
b) $ord(a) = ord(a^{-1})$.
c) ord(a) là bội của ord(f(a)).

31. Tìm tất cả các nhóm con của
a) Nhóm cyclic cấp 6.
b) Nhóm cyclic cấp 24.

32. Chứng minh rằng mọi nhóm có cấp ≤ 5 đều giao hoán .

33. Chứng minh rằng mọi nhóm giao hoán cấp 6 có chứa một phần tử cấp 3 đều là nhóm cyclic.

34. Chứng minh rằng nhóm thương của một nhóm cyclic là một nhóm cyclic.

35. Giả sử $(G, \bullet)$ là nhóm cyclic vô hạn có phần tử sinh là x. Với $m \in \angle$ đặt $H_m = \{ x^{km} : k \in 9 \}$. Chứng minh rằng
a) H_m là nhóm con của G.
b) Nếu $m \neq n$ thì $H_m \neq H_n$.
c) Mọi nhóm con của G đều có dạng H_m với m là một số tự nhiên nào đó.

36. Chứng minh rằng Int(G) (xem bài 13.) là chuẩn tắc trong Aut(G) .

37. Cho $(G, \bullet)$ là một nhóm; A và B là các nhóm con chuẩn tắc sao cho $A \cap B = \{1\}$. Chứng minh rằng $ab = ba$, với mọi $a \in A$, $b \in B$.

38

a) Cho (G, •) là một nhóm giao hoán, và H là nhóm con của G. Chứng minh rằng G/H là nhóm giao hoán.

b) Cho (G, •) là một nhóm, và H là nhóm con chuẩn tắc của G. Chứng tỏ rằng G/H là nhóm giao nếu và chỉ nếu $xyx^{-1}y^{-1} \in H$, với mọi x, y ∈ G.

c)Ta gọi $C(G) = \{ xyx^{-1}y^{-1}, x, y \in G\}$ là **nhóm con các hoán tử** của G, các phần tử của nó được gọi là các **hoán tử**. Chứng tỏ rằng C(G) là một nhóm con chuẩn tắc của G.

d) Chứng minh rằng G/C(G) là giao hoán.

39. Cho (G,•) là nhóm; A, B là các nhóm con chuẩn tắc trong G. Đặt $AB = \{ ab : a \in A ; b \in B \}$. Chứng minh rằng

a) AB là nhóm con của G.

b) A là nhóm con chuẩn tắc của AB, $A \cap B$ là nhóm con chuẩn tắc của B.

c) $AB/A \cong B/A \cap B$.

40. Cho (∀,+) là nhóm cộng các số phức, (3,+) là nhóm cộng các số thực và ánh xạ $f : (\forall ,+) \longrightarrow (3, +)$, $f(a + bi) = b ; a,b \in 3$.

a) Chứng minh rằng f là toàn cấu nhóm.

b) Xác định Kerf, ∀/Ker(f)

c) Chứng minh rằng ∀/3

41. Một phép đối xứng của một hình hình học là một phép thế của tập hợp X các điểm của hình đó và bảo toàn khoảng cách. Chứng minh rằng tập hợp các phép đối xứng của các hình hình học là một nhóm đối với phép hợp các ánh xạ.

42. Kí hiệu Δ_3 là nhóm đối xứng của một tam giác đều và gọi là nhóm tam giác đều.

a) Chứng minh rằng : $\Delta_3 = \{1, R, R^2, D_1, D_2, D_3 \}$.

Trong đó :

- R là phép quay tâm O, góc quay 120^0.
- D_i là phép đối xứng qua đường cao đi qua đỉnh thứ i.

b) Hãy lập bảng toán cho Δ_3. Suy ra rằng : $\Delta_3 \cong S_3$.

CHƯƠNG 4:
VÀNH VÀ TRƯỜNG

1. Vành và trường

1.1 Định nghĩa

• Cấu trúc đại số (X, +, •), trong đó + và • là hai phép toán trong trên X, được gọi là một **vành** nếu:

d) (X, +) là một nhóm giao hoán.
e) (X, •) là một vị nhóm.
f) Phép toán • phân phối đối với phép +.

• Phần tử đơn vị của nhóm (X,+) thường được kí hiệu 0_X. Phần tử đơn vị (kí hiệu là 1_X) của vị nhóm (X, •) cũng được gọi là **phần tử đơn vị của vành**. Một vành mà $0_X = 1_X$ được gọi là **vành tầm thường**. Nếu phép toán • có tính giao hoán thì vành (X, +. •) được gọi là **vành giao hoán**.

• Cho (X, +, •) là một vành, nó có thể xảy ra trường hợp rằng, tồn tại các phần tử a, b ∈ X sao cho a ≠ 0, b ≠ 0 (0 là phần tử đơn vị của nhóm (X,+)) nhưng ab = 0. Những phần tử như thế được gọi là **ước của không**. Một vành không tầm thường, giao hoán, không có ước của không được gọi là **vành nguyên** hoặc **miền nguyên**.

• Vành (X, +, •) được gọi là một **trường** nếu nó là không tầm thường, giao hoán và mọi phần tử khác 0 đều có nghịch đảo đối với phép toán • . Như vậy nếu (X, +, •) là một trường thì (X – {0}, •) là một nhóm.

• VÍ DỤ:
1) (9 ,+, •) là vành giao hoán, (Θ ,+,•),(3,+,•),(∀ ,+,•) là các trường, và tất cả đều là vành nguyên.

2) Cho (G,+) là nhóm giao hoán. Trên End(G) xác định hai phép toán + và o như sau, với x ∈ G

$$(g + f)(x) = g(x) + f(x) \quad \text{và} \quad (f \circ g)(x) = f(g(x)).$$

Khi đó (End(G),+, o) là một vành. Thật vậy, dễ kiểm tra rằng (End(G),+) là nhóm giao hóan với phần tử đơn vị là đồng cấu $x \mapsto 0$; (End(G), o) là vị nhóm với phần tử đơn vị là ánh xạ đồng nhất $x \mapsto x$. Tính phân phối của phép o đối với phép + được suy ra từ :

$$\begin{aligned}(fo(g + h))(x) &= f((g + h)(x)) \\ &= f(g(x) + h(x)) = f(g(x)) + f(h(x))\end{aligned}$$

$= (f \circ g)(x)) + (f \circ h)(x).$

3) Cho $(X,+,\bullet)$ là một vành và A là tập hợp khác rỗng. Gọi M(A,X) là tập tất cả các ánh xạ từ A đến X. Trên M(A,X), xác định hai phép toán cộng và nhân như sau, với mọi $x \in A$

$$(f + g)(x) = f(x) + g(x) \quad \text{và} \quad (f.g)(x) = f(x).g(x).$$

Khi đó $(M(A, X), +, \bullet)$ là một vành với phần tử đơn vị là ánh xạ $x \mapsto 1_X$, hơn nữa nó là giao hoán nếu X giao hoán.

4) $Mat_K(n)$ là một vành đối với các phép toán cộng và nhân ma trận.

5) $(9_n, +, \bullet)$ là một vành giao hoán, với các phép toán

$$\overline{m} + \overline{k} = \overline{m+k} \quad \text{và} \quad \overline{m}.\overline{k} = \overline{m.k}$$

Vành này được gọi là **vành các số nguyên modulo n.** Vành 9_6 không phải là vành nguyên vì $\overline{2}.\overline{3} = \overline{0}$. Vành 9_3 là một vành nguyên.

1.2 Các tính chất

Tính chất 1 Cho $(X,+,\bullet)$ là một vành. Khi đó, với mọi $x, y \in X$ và $n \in 9$ ta có

a) $x0 = 0 = 0x$.

b) $(-x).y = -x.y = x.(-y)$.

c) $(-x).(-y) = xy$

d) $n(x.y) = (nx).y = x.(ny)$.

Chứng minh :

a) Vì $x0 = x(0 + 0) = x0 + x0$ nên $x0 = 0$. Tương tự $0x = 0$

b) Vì $0 = 0.y = (-x + x).y = (-x).y + xy$ nên $(-x).y = -xy$

Vì $0 = x.0 = x.(-y + y) = x.(-y) + xy$ nên $x(-y) = -xy$

c) Từ b) suy ra $(-x).(-y) = x.[-(-y)] = xy$

d) . Với $n = 0$ là rõ ràng.

. Với $n \in \angle$: $n(a.b) = a.b + ... + a.b = \begin{cases} \underbrace{a.(b + \cdots + b)}_{n} = a.(nb). \\ \underbrace{(a + \cdots + a).b}_{n} = (na).b. \end{cases}$

. Với $n = -k, k \in \angle$

$$n(a.b) = (-k)(a.b) = -[k(a.b)] = \begin{cases} -[(ka)b] = [-(ka)b] = [(-k)a]b = (na)b. \\ -[a(kb)] = a[-(kb)] = a[(-k)b] = a(nb). \end{cases}$$ □

• NHẬN XÉT: Nếu (X, +, •) là vành tầm thường thì X = {0}. Thật vậy vì với mọi x ∈ X ta có x = 1.x = 0.x = 0.

Tính chất 2: Trong một miền nguyên (X, +, •) phép toán • thỏa mãn luật giản ước (tức là, từ a ≠ 0 và ab = ac kéo theo b = c)

Chứng minh: Giả sử có a ≠ 0 và ab = ac, khi đó a (b – c) = 0. Do a ≠ 0 và trong X không có ước của 0 nên b – c = 0 hay b = c (ở đây phép trừ b – c có nghĩa là b + (– c)). □

Tính chất 3: Mọi trường đều là vành nguyên.

Chứng minh: Giả sử có hai phần tử a, b của trường X sao cho ab = 0. Nếu a khác 0 thì do X là trường nên a có nghịch đảo a^{-1}. Từ $a^{-1}.a.b = a^{-1}.0 = 0$ ta suy ra b = 0 do luật giản ước trong nhóm nhân (X – {0}, •). □

• NHẬN XÉT: Một vành nguyên có thể không phải là một trường, chẳng hạn vành nguyên (9, +, •).

Tính chất 4: Mọi vành nguyên hữu hạn đều là trường.

Chứng minh: Giả sử vành nguyên X có n phần tử $a_1, a_2, \ldots, a_3$. Xét phần tử a ≠ 0 bất kì của X, và ánh xạ $f_a : X \to X$, $f_a(x) = ax$. Ta có f_a là đơn ánh vì nếu có $f_a(x) = f_a(x')$ tức là ax = ax' thì x = x' do luật giản ước trong X. Vì X là hữu hạn nên f_a cũng là song ánh. như vậy với $1_x \in X$ tồn tại b ∈ X sao cho $f_a(b) = ab = 1_x$, tức là b là nghịch đảo của a. □

2. Vành con – Trường con

2.1 Định nghĩa

• Cho (X,+,•) là một vành. Tập con S khác rỗng của X được gọi là một **vành con** của X nếu

a) S là tập con ổn định của X, tức là, $1_X \in S$ và nếu x, y ∈ S thì x + y và x.y cũng thuộc S.
b) (S, +, •) là một vành.

• Cho (X,+,•) là một trường. Tập con S khác rỗng của X được gọi là một **trường con** của X nếu

a) S là tập con ổn định của X, tức là, nếu x, y ∈ S thì x + y và x.y cũng thuộc S.

b) (S, +, •) là một trường.

• NHẬN XÉT:
1) Nếu S là trường con của trường X thì $1_X \in S$ vì khi đó (S,+) là nhóm con của (X,+) và (S – {0}, •) là một nhóm con của nhóm (X – {0}, •).

2) Bất kì một vành X nào cũng có hai vành con tầm thường là bản thân nó và vành không(chỉ gồm phần tử 0 của X)

2.2 Định lí (tiêu chuẩn nhận biết một vành con)

Tập con $S \neq \emptyset$ của vành X là vành con nếu và chỉ nếu

a) $1_X \in S$
b) Nếu $a, b \in S$ thì $a - b \in S$.
c) Nếu $a, b \in S$ thì $a.b \in S$.

Chứng minh :
($\Rightarrow$) : Hiển nhiên
($\Leftarrow$) : Từ b) suy ra (S, +) là nhóm con của (X,+) và do đó S là tập con ổn định của X. Mặt khác, vì phép • trong X có tính kết hợp nên nó cũng kết hợp trong S; phần tử đơn vị của X nằm trong S nên nó cũng là đơn vị của A. Vậy (A – {0} , •) là vị nhóm. Cuối cùng luật phân phối có hiệu lực trong X tất nhiên cũng có hiệu lực trong A.

Hòan toàn tương tự ta cũng có

2.3 Định lí (tiêu chuẩn nhận biết một trường con)

Tập con S chứa nhiều hơn một tử của trường X là trường con nếu và chỉ nếu

a) Nếu $a, b \in S$ thì $a - b \in S$.
b) Nếu $a, b \in S$ thì $a.b \in S$.
c) Nếu $a \in S$ và $a \neq 0$ thì $a^{-1} \in S$.

• CHÚ Ý: Điều kiện a), b) và c) trong định lí 2.3 có thể thay bởi điều kiện tương đương:

a') Nếu $a, b \in S$ thì $a - b \in S$.
b') Nếu $a, b \in S$ và $b \neq 0$ thì $a.b^{-1} \in S$.

• VÍ DỤ:
1) 9 là vành con của Θ, 3, ∀; Θ và 3 trường con của ∀.

2) $9[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in 9\}$ là một vành con của (3 , +, •).

3) $\Theta[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \Theta\}$ là một trường con của (3 , +, •).

4) Các hàm khả vi $f : 3 \to 3$ tạo thành một vành con của vành các hàm liên tục (với phép cộng và phép nhân các hàm số thông thường).

5) Nếu $\{A_i , i \in I\}$ là họ các vành con của X thì $\bigcap_{i\in I} A_i$ cũng là vành con của X.

Thật vậy, rõ ràng $1_X \in \bigcap_{i\in I} A_i$. Giả sử $x, y \in \bigcap_{i\in I} A_i$, khi đó $x, y \in A_i$, với mọi $i \in I$. Do A_i là vành con nên $x – y$ và $xy \in A_i$, với mọi $i \in I$. Từ đó suy ra $x – y$ và $xy \in \bigcap_{i\in I} A_i$. Vậy, theo 2.2, $\bigcap_{i\in I} A_i$ cũng là vành con của X.

3. Ideal - Vành thương

3.1 Định nghĩa

• Cho (X,+, •) là một vành và A là một tập con khác rỗng của X. Khi đó A được gọi là **ideal** của X nếu ba điều kiện sau được thỏa mãn:

1) (A,+) là nhóm con của (X,+).
2) $ax \in A$ và $xa \in A$ với mọi $a \in A$, với mọi $x \in X$.

• VÍ DỤ:

1) Cho (X,+, •) là vành, khi đó {0} và X là các ideal của X, chúng được gọi là các **ideal tầm thường** của X.

2) Cho (X,+, •) là một vành giao hoán và b là một phần tử của X. Khi đó tập hợp $Xb = \{ xb : x \in X \}$ là ideal của X.

3) Xét C [0,1] là vành các hàm liên tục trên đoạn [0,1]. Đặt J là tập tất cả các hàm $f \in C [0,1]$ sao cho $f(\frac{1}{2}) = 0$. Khi đó J là một ideal của C [0,1].

4) Xét vành số nguyên (9, +, •) và J là tập các số nguyên chẵn. Khi đó J là một ideal của 9. Tập các số nguyên lẻ có phải là ideal của 9 không? Tập hợp $m 9$ gồm các bội số của m là một ideal của 9.

5) Nếu A và B là các ideal của vành X, thì tập $A + B = \{a + b : a \in A, b \in B\}$ là một ideal của X.

6) Nếu A, B là các ideal của vành X, thì $AB = \{ \sum_{i=1}^{n} a_i b_i : a_i \in A, b_i \in B, n \in \angle \}$ là một ideal của X

7) Nếu $\{A_i , i \in I\}$ là họ các ideal của X thì $A = \bigcap_{i\in I} A_i$ cũng là ideal của X.

Thật vậy, trước hết $A \neq \varnothing$ vì có ít nhất phần tử 0 của vành X thuộc tất cả các ideal A_i, và do đó nó thuộc A. Giả sử x, y $\in$ A, khi đó x, y $\in A_i , \forall$ i $\in$ I. Do A_i là nhóm con nên x – y $\in A_i$, với mọi i $\in$ I, từ đó x – y $\in$ A. Vậy (A,+) là một nhóm con. Bây giờ giả sử a là một phần tử bất kì của A và x là một phần tử của X, ta có a $\in$ A nên a $\in A_i , \forall$ i $\in$ I, mà A_i là ideal nên xa và ax thuộc A_i, với mọi i, từ đó xa và ax thuộc A. Như vậy A là một ideal.

• CHÚ Ý:

1) Nếu ideal A của vành X chứa phần tử đơn vị 1_X thì A = X. Thật vậy, vì với mọi x $\in$ X ta có x = x.1 $\in$ A, tức là X $\subset$ A.

2) Giả sử X là một vành giao hoán không tầm thường. Khi đó X là một trường khi và chỉ khi X không có ideal nào ngoại trừ các ideal tầm thường. Thật vậy, giả sử X là một trường. Nếu I là ideal khác {0} thì I chứa một phần tử a $\neq$ 0, do X là trường nên tồn tại phần tử nghich đảo $a^{-1} \in$ X. Vì 1 = a.$a^{-1} \in$I nên theo chú ý 1) ở trên I = X. Ngược lại, giả sử X không có ideal nào ngoại trừ các ideal tầm thường. Gọi a là một phần tử khác 0 bất kì của X. Dễ kiểm tra rằng tập hợp X.a = {xa, x $\in$ X} là một ideal của X. Vì X.a $\neq$ {0} nên X.a = X, từ đó với 1 $\in$X, tồn tại a' $\in$X sao cho a' a = a a' = 1, tức là a' = a^{-1}.

3. 2 Ideal chính

• Cho X là một vành giao hóan , S là một tập con của X. Khi đó, giao của các ideal của X chứa S là một ideal chứa S, và nó là ideal nhỏ nhất của vành X chứa tập S. Ideal này sẽ được gọi là **ideal sinh ra bởi tập S** và ký hiệu < S >.

• Nếu S = $\{a_1, a_2,...., a_n\}$ thì < S > được gọi là **ideal sinh ra bởi các phần tử a_1, a_2,...., a_n.** Có thể chỉ ra rằng

$$< a_1, a_2,...., a_n > = \{x_1a_1 + x_2 a_2 +....+x_na_n : x_1, x_2, ...,x_n \in X \}$$

• Nếu S chỉ gồm một phần tử a thì ideal sinh bởi một phần tử a được gọi là **ideal chính**.

3. 3 Vành thương

• Giả sử (X,+, •) là một vành và I là một ideal của X. Khi đó, (I,+) là nhóm con giao hóan của (X,+). Nhóm thương X / I = {x + I | x $\in$ X } cũng là nhóm giao hóan (xem mục nhóm thương), với phép tóan cộng xác định như sau

$$(x + I) + (y + I) = (x + y) + I.$$

Bây giờ ta muốn trang bị trên X / I một phép tóan nhân để nó trở thành một vành. Giả sử $x + I$ và $y + I$ là hai phần tử bất kì của X / I, ta định nghĩa phép nhân giữa chúng như sau

$$(x + I).(y + I) = x.y + I.$$

Dễ thấy rằng qui tắc này không phụ thuộc đại diện của các lớp $x + I$, $y + I$, nó có tính kết hợp, phân phối đối với phép cộng và có phần tử đơn vị là $1 + I$. Vậy $(X / I,+, \bullet)$ là một vành, nó được gọi là **vành thương của X trên I**.

• VÍ DỤ:
1) Nếu $I = \{0\}$ thì $X /\{0\} = \{x + \{0\}\} = X$.
2) Nếu $I = X$ thì $X / X = \{x + X : x \in X\} = \{X\}$, vành thương trong trường hợp này là vành tầm thường, nó chỉ chứa có một phần tử đơn vị là X.

3) Xét vành các số nguyên 9 và m 9 là ideal của 9. Vành thương của 9 trên m 9 là

$$9_m = {}^{9}/_{m9} = \{\bar{0}, \bar{1}, \ldots, \overline{m-1}\}$$

với các phép toán $\bar{p} + \bar{q} = \overline{p+q}$ và $\bar{p}.\bar{q} = \overline{p.q}$

4. Đồng cấu vành

4.1 Định nghĩa

• Cho $(X,+, \bullet)$,$(Y,+, \bullet)$ là các vành. Ánh xạ $f : X \to Y$ được gọi là một **đồng cấu vành** nếu với mọi $a, b \in X$, các điều sau được thỏa mãn

1) $f(a + b) = f(a) + f(b)$
2) $f(a.b) = f(a). f(b)$
3) $f(1_X) = 1_Y$

• Đồng cấu vành f được gọi là **đơn cấu**, **tòan cấu**, **đẳng cấu** nếu f lần lượt là đơn ánh, tòan ánh, song ánh. Nếu giữa $(X,+,\bullet)$ và $(Y,+,\bullet)$ tồn tại một đẳng cấu vành, thì ta nói chúng đẳng cấu với nhau, và viết $X \cong Y$.

• NHẬN XÉT: Nếu $f : (X,+,\bullet) \to (Y,+,\bullet)$ là một đồng cấu vành thì $f : (X,+) \to (Y,+)$ là đồng cấu nhóm.

• VÍ DỤ:
1) Cho $(X, +, \bullet)$ khi đó ánh xạ đồng nhất $id :X \to X$ là một đẳng cấu vành.

2) Ánh xạ $f : (9 ,+, \bullet) \rightarrow (9_n,+, \bullet)$, $f(m) = \overline{m}$, là toàn cấu vành.

3) Cho $(X, +, \bullet)$ là một vành và End(X) là vành các đồng cấu của nhó $(X,+)$. Khi đó ánh xạ $f : (X, +, \bullet) \rightarrow (End(X), +, \bullet)$, $a \mapsto f_a$ với $f_a(x) = a.x$ là một đồng cấu vành.

4) Giả sử I là một ideal của vành X. Xét ánh xạ

$$\pi : X \rightarrow X / I, \ \pi (x) = x + I$$

π là một toàn cấu vành, gọi là **toàn cấu chính tắc.**

4.2 Các tính chất của đồng cấu vành

Các tính chất sau đây là tương tự như trong nhóm mà việc chứng minh nó là tương tự hoặc được trực tiếp suy ra từ kết quả về đồng cấu nhóm.

• *Tính chất 1* Hợp của hai đồng cấu vành là một đồng cấu vành. Hơn nữa hợp của hai đẳng cấu là một đẳng cấu.

• *Tính chất 2* Cho $(X,+, \bullet)$ và $(Y,+, \bullet)$ là các vành và $f : X \rightarrow Y$ là một đồng cấu vành. Khi đó

a) Nếu A là vành con (tương ứng : ideal) của X thì f(A) là vành con (tương ứng : ideal) của Y.

b) Nếu B là vành con (tương ứng : ideal) của Y thì $f^{-1}(B)$ là vành con (tương ứng : ideal) của X.

Đặc biệt ta có $Ker f = \{x \in X : f(x) = 0_Y\}$ là một ideal của X .

• *Tính chất 3* Cho $(X,+, \bullet)$ và $(Y,+, \bullet)$ là các vành và $f : X \rightarrow Y$ là một đồng cấu vành. Khi đó

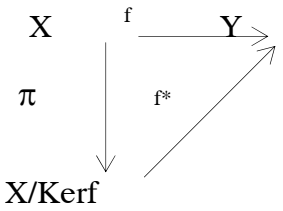
c) f là đơn cấu khi và chỉ khi $Kerf = \{0_X\}$.

d) f là toàn cấu khi và chỉ khi $Imf = Y$.

Tương tự như trường hợp đồng cấu nhóm, ở đây cũng có định lí cơ bản của đồng cấu vành như sau:

4.3 Định lí (cơ bản của đồng cấu vành)

Cho f là một đồng cấu từ vành X đến vành Y và $\pi : X \to X/Kerf$ là toàn cấu chính tắc từ vành X đến vành thương X / kerf . Khi đó tồn tại duy nhất một đồng cấu $f^* : X / kerf \to Y$ sao cho $f = f^* o\ \pi$, tức là biểu đồ sau giao hoán:



Hơn nữa, f^* là một đơn cấu và $Im\ f^* = f(X) = Imf$

4.4 Hệ quả

3) Với mọi đồng cấu vành $f : X \to Y$ ta có $f(X) \cong X/Kerf$
4) Với mọi toàn cấu nhóm $f : X \to Y$ ta có $Y \cong X/Kerf$.

4.5 Đặc số của vành

• Một vành không tầm thường X được gọi là có **đặc số** m nếu và chỉ nếu m là số nguyên không âm nhỏ nhất sao cho m.1 = 0.

• VÍ DỤ: Vành số nguyên 9 có đặc số 0, vành $^9/_{m\,9}$ có đặc số m.

• NHẬN XÉT: Nếu vành không tầm thường X có đặc số m thì cấp của mọi phần tử của nhóm (X, +) là một ước của m. Thật vậy, với mọi $a \in X$ và n là cấp của nó, khi đó ta có m.a = m(1.a) = (m.1)a = 0.a = 0. Chia m cho n ta được $m = nq + r$, $0 \le r < n$. Nếu $r > 0$ thì từ $ma = (nq + r)a = (nq)a + ra = 0$ suy ra $ra = 0$, nhưng điều này mâu thuẩn với tính chất bé nhất của n. Vậy phải có $r = 0$, tức là $n \mid m$.

• CHÚ Ý: Ta hiểu một đồng cấu f (đơn cấu, tòan cấu, đẳng cấu) từ trường X đến trường Y như là một đồng cấu (đơn cấu, tòan cấu, đẳng cấu) vành. Vì trong trường không có ideal nào khác ngòai các ideal tầm thường nên ta có hoặc kerf = {0} hoặc kerf = X. Trường hợp kerf = {0} thì f là một đơn cấu. Còn trường hợp kerf = X thì f là đồng cấu không. Vậy mọi đồng cấu trường hoặc là đơn cấu hoặc là đồng cấu không.

5. Các định lí nhúng đẳng cấu

5.1 Định lí (nhúng đẳng cấu một vị nhóm)

Giả sử X là một vị nhóm giao hoán với phần tử đơn vị là e. S là tập hợp tất cả các phần tử chính qui của X (một phần tử $a \in X$ gọi là phần tử **chính qui** nếu với mọi

b, c $\in$ X sao cho ab = ac hoặc ba = ca thì b = c). Khi đó có một vị nhóm giao hoán $\overline{X}$ và một đơn cấu f từ X đến $\overline{X}$ thỏa các tính chất sau

a) Mọi phần tử của f(S) đều có nghịch đảo trong $\overline{X}$.
b) Các phần tử của $\overline{X}$ có dạng $f(x).[f(a)]^{-1}$ với $x \in X$ và $a \in S$.

Chứng minh:
1) Xây dựng vị nhóm $\overline{X}$. Trên tập tích $X \times S$, ta xác định một quan hệ tương đương R như sau

$$(x, a)\ R\ (y, b) \Leftrightarrow xb = ay$$

Tính phản xạ, đối xứng là rõ ràng. Giả sử có (x, a)R(y, b) và (y, b)R(z, c), tức là xb = ay và yc = bz, từ đó xbc = abz. Vì b chính qui nên suy ra xc = az, tức là (x, a)R(z, c). Vậy R là bắc cầu.

Đặt $\overline{X}$ là tập thương $(X \times S)/R$ mà các phần tử của nó được kí hiệu là $\overline{(x,a)}$. Trên $\overline{X}$ ta xác định phép toán trong như sau

$$\overline{(x,a)}.\overline{(y,b)} = \overline{(xy,ab)}$$

Định nghĩa không phụ thuộc vào đại diện của các lớp tương đương. Thật vậy, giả sử (x,a) R (x',a') và (y,b) R (y',b'), tức là xa' = ax' và yb' = by' thì suy ra xya'b' = x'y' ab, tức là $\overline{(xy,ab)} = \overline{(x'y',a'b')}$.

Khi đó có thể kiểm tra rằng $\overline{X}$ là vị nhóm giao hoán, với phần tử đơn vị là $\overline{(e,e)}$.

2) Đơn cấu $f : X \to \overline{X}$ được xác định bởi $f(x) = \overline{(x,e)}$.
f là đồng cấu vì $f(xy) = \overline{(xy,e)} = \overline{(x,e)}\,\overline{(y,e)} = f(x)f(y)$, f là đơn ánh vì từ f(x) = f(y) suy ra $\overline{(x,e)} = \overline{(y,e)}$, từ đó (x, e)R(y, e) hay xe = ye, suy ra x = y.

3) Cặp $(\overline{X}, f)$ thỏa mãn các tính chất nêu trong định lí. Thật vậy, với $x \in S$ phần tử nghịch đảo của $f(x) = \overline{(x,e)}$ là $\overline{(e,x)}$ vì $\overline{(x,e)}.\overline{(e,x)} = \overline{(x,x)} = \overline{(e,e)}$. Ngòai ra mỗi phần tử $\overline{(x,a)}$ của $\overline{X}$ có thể viết
$\overline{(x,a)} = \overline{(x,e)}.\overline{(e,a)} = \overline{(x,e)}\,(\overline{(a,e)})^{-1} = f(x).[f(a)]^{-1}$. □

• NHẬN XÉT:

1) Nếu mọi phần tử của vị nhóm X đều là chính qui thì tất cả các phần tử của $\overline{X}$ đều có phần tử nghịch đảo nên $\overline{X}$ là một nhóm. Mặt khác , vì $f : X \to \overline{X}$ là một đơn cấu nên $X \cong f(X) = \{\overline{(x,e)}, x \in X\} \subset \overline{X}$, trong trường hợp này ta cũng nói

rằng **vị nhóm X được nhúng đẳng cấu vào nhóm** $\overline{X}$, và có thể đồng nhất phần tử $x \in X$ với phần tử $f(x) = \overline{(x,e)} \in \overline{X}$. Mọi phần tử của $\overline{X}$ do đó viết được dưới dạng $x.y^{-1}$ với $x, y \in X$.

2) Ta có thể chứng minh được rằng cặp $(\overline{X}, f)$ là duy nhất theo nghĩa sai khác nhau một đẳng cấu, nghĩa là nếu có một cặp (Y, g) khác thỏa mãn a) và b) trong định lí thì có một đẳng cấu $\varphi : \overline{X} \to Y$ và $g = \varphi \circ f$. Thật vậy ta xét tương ứng $t = f(x).[f(a)]^{-1} \mapsto g(x).[g(a)]^{-1}$. Tương ứng này là một ánh xạ vì nếu có $f(x).[f(a)]^{-1} = f(x').[f(a')]^{-1}$, tức là $f(x)f(a') = f(x')f(a)$, hay, do f là đồng cấu, $f(xa') = f(x'a)$, từ đó $xa' = x'a$ (vì f đơn ánh) và do g là đồng cấu ta suy ra $g(xa') = g(x'a)$, $g(x)g(a') = g(x')g(a)$, $g(x).[g(a)]^{-1} = g(x').[g(a')]^{-1}$. Dễ dàng chỉ ra φ là một đẳng cấu và $g = \varphi \circ f$.

- ÁP DỤNG:

1) *Số nguyên.* Áp dụng định lí trên cho $X = (\angle_0, +)$. Vì mọi phần tử của $\angle_0$ đều chính qui nên $\overline{X}$ là một nhóm mà ta kí hiệu nó 9. Các phần tử của 9 có dạng $\overline{(n,m)}$, với $m, n \in \angle_0$, được gọi là các số nguyên và phép cộng trên 9 được xác định bởi

$$\overline{(n,m)} + \overline{(p,q)} = \overline{(n+p, m+q)}$$

Mỗi số nguyên có thể viết dưới dạng $m - n := m + (-n)$, với $m, n \in \angle_0$.

2) *Số hữu tỉ dương.* Áp dụng định lí trên cho $X = (\angle, \bullet)$. Vì mọi phần tử của $\angle$ đều chính qui nên $\overline{X}$ là một nhóm mà ta kí hiệu nó Θ_+. Các phần tử của Θ_+ có dạng $\overline{(n,m)}$, với $m, n \in \angle$, được gọi là các số hữu tỉ dương và phép nhân trên Θ_+ được xác định bởi

$$\overline{(n,m)}.\overline{(p,q)} = \overline{(np, mq)}$$

Mỗi số hữu tỉ dương có thể viết dưới dạng $\frac{p}{q} := p.q^{-1}$, với $p, q \in \angle$.

5.2 Định lí (nhúng đẳng cấu một vành nguyên)

Giả sử X là một vành nguyên với phần tử đơn vị là 1. X^* là tập hợp tất cả các phần tử khác 0 của X. Khi đó có một trường $\overline{X}$ và một đơn cấu (vành) f từ X đến $\overline{X}$ thỏa các tính chất sau

a) Mọi phần tử của $f(X^*)$ đều có nghịch đảo trong $\overline{X}$.
b) Các phần tử của $\overline{X}$ có dạng $f(x).[f(a)]^{-1}$ với $x \in X$ và $a \in X^*$.

Chứng minh:
. Vì (X, +, •) là vành nguyên nên (X, •) là một vị nhóm giao hoán, và X^* là tập các phần tử chính qui. Gọi $\overline{X}$ là vị nhóm nhân giao hoán được xây dựng như trong định lí 5.1, với phép toán như sau

$$\overline{(x,a)}.\overline{(y,b)} = \overline{(xy,ab)}$$

. Bây giờ trong $\overline{X}$ xác định thêm một phép toán cộng như sau:

$$\overline{(x,a)} + \overline{(y,b)} = \overline{(xb+ay,ab)}$$

Phép toán này được xác định không phụ thuộc vào việc chọn các đại diện của lớp tương đương. Thật vậy, giả sử (x, a) R (x', a') và (y, b) R (y', b'), tức là

$$xa' = ax' \quad \text{và} \quad yb' = by'$$

thì suy ra $xa'bb' = ax'bb'$ và $yb'aa' = by'aa'$

Cộng hai đẳng thức này vế theo vế $(xb + ay)a'b' = (x'b' + a'y')ab$

tức là $\overline{(xb+ay,ab)} = \overline{(x'b'+a'y',a'b')}$

. Khi đó có thể kiểm tra rằng $(\overline{X}, +)$ là một nhóm giao hoán, phần tử đơn vị là $0 = \overline{(0,1)}$, phần tử nghịch đảo của $\overline{(x,a)}$ là $\overline{(-x,a)}$, $(\overline{X} - \{0\}, \bullet)$ như đã biết là một vị nhóm giao hoán, hơn nữa mọi phần tử $\overline{(x,a)} \neq 0$ đều có nghịch đảo là $\overline{(a,x)}$. Ngòai ra phép nhân có tính chất phân phối đối với phép cộng. Như vậy $(\overline{X}, +, \bullet)$ là một trường.

. Xét ánh xạ $f : X \to \overline{X}$ được xác định bởi $f(x) = \overline{(x,1)}$. Như đã biết f là một đơn ánh thỏa f(xy) = f(x).f(y), hơn nữa $f(x + y) = \overline{(x+y,1)} = \overline{(x,1)} + \overline{(y,1)} = f(x) + f(y)$. Như vậy f là một đơn cấu vành.

3) Cặp $(\overline{X}, f)$ thỏa mãn các tính chất nêu trong định lí. Thật vậy, với $x \in X^*$ phần tử nghịch đảo của $f(x) = \overline{(x,1)}$ là $\overline{(1,x)}$. Ngòai ra mỗi phần tử $\overline{(x,a)}$ của $\overline{X}$ có thể viết $\overline{(x,a)} = \overline{(x,1)}.\overline{(1,a)} = \overline{(x,1)}\,(\overline{(a,1)})^{-1} = f(x).[f(a)]^{-1}$. □

• CHÚ Ý: 1) Ta cũng có thể chứng minh được rằng cặp $(\overline{X}, f)$ là duy nhất theo nghĩa sai khác nhau một đẳng cấu.

2) Vì $f : X \to \overline{X}$ là một đơn cấu nên $X \cong f(X) = \{\overline{(x,1)}, x \in X\} \subset \overline{X}$, trong trường hợp này ta cũng nói rằng **vành nguyên X được nhúng đẳng cấu vào trường** $\overline{X}$,

và có thể đồng nhất phần tử $x \in X$ với phần tử $f(x) = \overline{(x,1)} \in \overline{X}$. Mọi phần tử của $\overline{X}$ do đó viết được dưới dạng $\frac{x}{y} := x.y^{-1}$ với $x \in X$ và $y \in X^*$.

Mỗi phần tử của $\overline{X}$ còn được gọi là một **phân thức**. Trường $\overline{X}$ do đó còn được gọi là **trường các phân thức** hay **trường các thương** của vành nguyên X. Thỉnh thoảng ta cũng viết $\overline{X} = (X^*)^{-1}X$ (trong đó $X^* = X - \{0\}$) để chỉ trường các thương của vành nguyên X.

• VÍ DỤ: Áp dụng định lí cho vành nguyên 9. Trường các phân thức của 9 được kí hiệu là Θ. Các phần tử của Θ được gọi là các **số hữu tỉ**. Như vậy mỗi số hữu tỉ có thể viết dưới dạng $m\,n^{-1}$ hoặc $\frac{m}{n}$ với $m \in 9$ và $n \in 9^*$.

6. Số học trên vành nguyên - Vành chính - Vành Euclide - Vành Gauss

Trong suốt mục này ta giả thiết D là một miền nguyên với phần tử đơn vị là 1 và dùng kí hiệu D^* để chỉ tập hợp $D - \{0\}$.

6.1 Các định nghĩa

• Cho a, b là hai phần tử của D. Ta nói rằng a **là ước của** b (hoặc a **chia hết** b, hoặc b **là bội của** a, hoặc **b chia hết cho** a), kí hiệu $a \mid b$ nếu tồn tại một phần tử $c \in D$ sao cho $b = ac$.

• Nếu $a \in D^*$ là ước của đơn vị (tức là $a \mid 1$) thì a được gọi là **phần tử khả nghịch** của D.

• Hai phần tử $a, b \in D^*$ gọi là **liên kết với nhau**, kí hiệu $a \sim b$, nếu $a \mid b$ và $b \mid a$.

• Cho a là ước của b, khi đó a được gọi là **ước thực sự của b**, kí hiệu $a \parallel b$ nếu a không khả nghịch và không liên kết với b. Như vậy các phần tử khả nghịch và các phần tử liên kết với b không là ước thực sự của b, còn các ước khác của b là ước thực sự của b.

VÍ DỤ: Trong vành nguyên 9, các phần tử khả nghịch là ± 1. Phần tử a liên kết với phần tử b khi và chỉ khi $a = \pm b$. Số nguyên 8 có các ước thực sự là $\pm 2, \pm 4$ còn $\pm 1, \pm 8$ không phải là ước thực sự của 8.

• Phần tử $p \in D^*$ được gọi là **phần tử nguyên tố** nếu p không khả nghịch và thỏa mãn tính chất : $p \mid ab$ kéo theo $p \mid a$ hoặc $p \mid b$.

• Phần tử $p \in D^*$ được gọi là **phần tử bất khả qui** nếu p không khả nghịch và không có ước thực sự . Nói khác đi, $p \in D^*$ là bất khả qui nếu p không khả nghịch và thỏa mãn tính chất : $p = ab$ kéo theo $a \mid 1$ hoặc $b \mid 1$.

• Nếu $d \mid a_i$ với mọi i = 1, 2, …, n thì d được gọi là **ước chung** của các phần tử a_1 , a_2, …, a_n. Phần tử d được gọi là **ước chung lớn nhất** của a_1 , a_2, …, a_n nếu d là ước chung của a_1 , a_2, …, a_n và mọi ước chung khác của a_1 , a_2, …, a_n đều là ước của d. Ta cũng sử dụng kí hiệu $(a_1, a_2, \ldots, a_n)$ để chỉ ước chung lớn nhất của a_1 , a_2, …, a_n.

NHẬN XÉT : Hai ước chung lớn nhất của $a_1, a_2, \ldots, a_n$ là liên kết.

• Các phần tử a_1 , a_2, …, a_n được gọi là **nguyên tố cùng nhau** nếu chúng nhận 1 làm ước chung lớn nhất.

6.2 Các tính chất

1) $a \mid a$ và $a \mid 0$ với mọi $a \in D$.
2) $1 \mid a$ với mọi $a \in D$
3) Nếu $a \mid b$ và $b \mid c$ thì $a \mid c$.
4) Nếu $a \mid b$ thì $a \mid bc$.
5) Nếu $a \mid b$ và $c \mid d$ thì $ac \mid bd$.
6) Nếu $a \mid b_i$ với mọi i = 1, 2, …, n thì $a \mid \sum_{i=1}^{n} m_i b_i$, $m_i \in D$.

7) Nếu a khả nghịch thì $a \mid b$ với mọi $b \in D^*$.
8) Nếu tích $a_1a_2 \ldots a_n$ khả nghịch thì từng nhân tử của nó cũng khả nghịch.
9) Quan hệ liên kết là một quan hệ tương đương.
10) Hai phần tử liên kết với nhau khi và chỉ khi chúng sai khác nhau một nhân tử khả nghịch.
11) Hai phần tử khả nghịch thì liên kết.

12) Nếu p là bất khả qui thì các ước của p hoặc là khả nghịch hoặc là liên kết với p.
13) Mọi phần tử nguyên tố đều bất khả qui.

14) $< b > \subset < a > \Leftrightarrow a \mid b$ ($< b >$ là ideal sinh bởi b)
15) $< b > = < a > \Leftrightarrow a \sim b$
16) $< b > = D \Leftrightarrow b \mid 1$

Chứng minh:

Từ tính chất 1) đến 9) là dễ dàng suy ra từ định nghĩa. Ta chứng minh từ 10) đến 16).
10) Giả sử $a \sim b$, tức là $a \mid b$ và $b \mid a$, suy ra $b = am$ và $a = bn$, từ đó $b = bmn$, suy ra $mn = 1$, vậy m và n là khả nghịch. Ngược lại, giả sử $b = am$ với m là khả nghịch, khi đó ta cũng có $a = bm^{-1}$, tức là $a \mid b$ và $b \mid a$, hay $a \sim b$.

11) Giả sử a, b là khả nghịch và gọi a^{-1}, b^{-1} lần lượt là các nghịch đảo của chúng. Khi đó, $aa^{-1} = 1 = bb^{-1}$, suy ra $a = b\,b^{-1}a$ và $b = aa^{-1}b$, tức là $a \mid b$ và $b \mid a$, hay $a \sim b$.

12) Giả sử a là ước của p, tức là ta có $p = ab$. Vì p là bất khả qui nên $a \mid 1$ hoặc $b \mid 1$. Do đó, nếu a không khả nghịch thì b phải khả nghịch, gọi b^{-1} là nghịch đảo của b, khi đó ta có $a = pb^{-1}$, tức là $a \mid p$ và $p \mid a$, hay $a \sim p$.

13) Giả sử $p = ab$, suy ra $p \mid ab$. Vì p là nguyên tố nên $p \mid a$ hoặc $p \mid b$. Nếu $p \mid a$, tức là $a = pu = abu$, thì $bu = 1$, suy ra $b \mid 1$. Tương tự nếu $p \mid b$ thì $a \mid 1$.

14) Giả sử $< b > \subset < a >$, khi đó $b \in < a >$ nên $b = xa$ với $x \in D$ nào đó, suy ra $a \mid b$. Ngược lại giả sử $a \mid b$. Gọi t là phần tử bất kì của $< b >$, khi đó ta có $t = bx = arx$, tức là $t \in < a >$. Vậy $< b > \subset < a >$.

15) và 16) suy ra trực tiếp từ 14) với chú ý rằng $< 1 > = D$. □

6.3 Vành chính

- Miền nguyên D được gọi là **vành chính** nếu mọi ideal của D đều là ideal chính.

- VÍ DỤ: $(\mathbb{Z}, +, \bullet)$ là vành chính. Thật vậy giả sử I là một ideal của $\mathbb{Z}$. Nếu $I = \{0\}$ thì $I = < 0 >$. Nếu $I \neq \{0\}$ thì nó chứa ít nhất một số nguyên dương (vì có $a, -a \in I$ với $a \neq 0$). Gọi n là số nguyên dương bé nhất trong I. Khi đó ta có $I = n\mathbb{Z}$. Thật vậy, giả sử y là số nguyên bất kì trong I. Chia y cho n ta được $y = nq + r$, $0 \leq r < n$. Vì $(I, +)$ là nhóm con nên $r = y - nq \in I$. Do tính bé nhất của n suy ra $r = 0$. Vậy $y = nq$, tức là $I \subset n\mathbb{Z}$. Bao hàm thức ngược lại $n\mathbb{Z} \subset I$ là hiển nhiên.

6.4 Định lí

Trong một vành chính D, ƯCLN d của n phần tử $a_1, a_2, ..., a_n$ bất kì luôn luôn tồn tại.

Chứng minh: Đặt $J = < a_1, ..., a_n > = \{ x_1a_1 + ... + x_na_n$; với $x_i \in D\}$. Vì D là vành chính nên tồn tại $d \in D$ sao cho $J = < d >$, thế thì tồn tại những $s_i \in D$ sao cho

$$d = s_1 a_1 + ... + s_n a_n$$

Ta có d là ước chung của a_1 ,...,a_n, thật vậy, vì $a_i = 0a_1 +\ldots+ 1a_i +...+ 0a_n \in J$ nên $a_i \in < d >$, và do đó $d \mid a_i$.

Giả sử c là một ước chung của a_1 ,...,a_n, tức là $a_i = cu_i$ với $u_i \in D$. Từ đó

$$d = s_1 a_1 +...+ s_n a_n = (s_1 u_1 + s_2 u_2 +\ldots+s_n u_n)c .$$

Suy ra $c \mid d$, và do đó d là ƯCLN của $a_1, a_2, ..., a_n$ □

6.5 Định lí

Trong một vành chính D ta có

1) Nếu e là ƯCLN của $a_1, a_2, ..., a_n$ thì tồn tại các $x_i \in D$ sao cho

$$e = x_1 a_1 +...+ x_n a_n$$

2) Các phần tử $a_1, a_2, ..., a_n$ là nguyên tố cùng nhau khi và chỉ khi tồn tại các $x_i \in D$ sao cho

$$x_1 a_1 +...+ x_n a_n = 1.$$

3) Nếu $c \mid ab$ mà c và a là nguyên tố cùng nhau thì $c \mid b$.
4) Nếu p là bất khả qui thì với bất kì $a \in D^*$ ta có hoặc $p \mid a$ hoặc p và a là nguyên tố cùng nhau.
5) Khái niệm phần tử bất khả qui và khái niệm nguyên tố là trùng nhau.

Chứng minh :
1) Xét ƯCLN d của của $a_1, a_2, ..., a_n$ của định lí 6.4, $d = s_1 a_1 +...+ s_n a_n$ (1)
Khi đó d liên kết với e, từ đó có một phần tử khả nghịch v sao cho e = dv. Nhân hai vế của (1) với v ta được:

$$e = dv = vs_1 a_1 +...+ vs_n a_n = x_1 a_1 +...+ x_n a_n, \text{ với } x_i = vs_i.$$

2) Suy ra trực tiếp từ 1)

3) Theo 2) tồn tại $r, s \in D$ sao cho $1 = as + cr$, suy ra $b = bas +bcr$. Mặt khác vì $c \mid ab$ nên tồn tại t để $ab = ct$. Do đó $b = cts + bcr = (ts + br)c$, tức là $c \mid b$.

4) Vì p là bất khả qui nên các ước của p hoặc là phần tử khả nghịch hoặc là liên kết với p. Do đó (p, a) chỉ có thể khả nghịch hoặc liên kết với p. Trong trường hợp đầu p và a là nguyên tố cùng nhau. Trong trường hợp sau $p \mid a$.

5) Ta đã có nếu p nguyên tố thì p bất khả qui. Bây giờ giả sử p là bất khả qui và $p \mid ab$. Theo 4) ta có hoặc $p \mid a$ hoặc $(p, a) =1$. Nhưng nếu $(p, a) = 1$ thì ta có do 3) $p \mid b$. Vậy p là nguyên tố. □

6.6 Vành Euclide

• Một vành nguyên D được gọi là **vành Euclide** nếu tồn tại một ánh xạ $g : D^* \to \angle$ thỏa các điều kiện

1) $g(ab) \geq g(a)$ với mọi $a, b \in D^*$;
2) Với mọi $a, b \in D$ và $b \neq 0$ tồn tại $q, r \in D$ sao cho

$$a = bq + r \quad \text{với } r = 0 \text{ hoặc } g(r) < g(b).$$

Điều kiện 2) là điều kiện xác định phép chia có dư của phần tử a cho phần tử $b \neq 0$, r được gọi là phần dư của phép chia. Phép chia gọi là chia hết nếu r = 0.

• VÍ DỤ: $(9, +, \bullet)$ là vành Euclide, ánh xạ g trong trường hợp này được xác định bởi $g(n) = |n|$.

6.7 Định lí

Mọi vành Euclide đều là vành chính

Chứng minh: Ta chứng minh mọi ideal I của vành Euclide D là chính. Thật vậy, nếu $I = \{0\}$ thì I là Ideal sinh bởi 0. Giả sử $I \neq \{0\}$. Gọi a là phần tử khác 0 của I sao cho g(a) bé nhất trong tập $g(I^*)$ (ở đây g là ánh xạ trong định nghĩa 6.6, và $I^* = I - \{0\}$). Ta sẽ chỉ ra $I = < a >$. Thật vậy, gọi x là một phần tử bất kì của I. Vì D là vành Euclide nên tồn tại $q, r \in D$ sao cho $x = aq + r$ với $r = 0$ hoặc $g(r) < g(a)$. Do $a, x \in I$ nên $r = x - aq \in I$. Nếu $r \neq 0$ thì ta có $r \in I^*$ và $g(r) < g(a)$. Nhưng điều này trái với tính chất của phần tử a. Vậy phải có r = 0, suy ra $x = aq \in < a >$, từ đó $I \subset < a >$. Bao hàm ngược lại là hiển nhiên. □

NHẬN XÉT: Từ 6.4 và 6.7 ta thấy trong vành Euclide hai phần tử bất kì đều có UCLN. Nhưng trong vành Euclide ta còn có thể chỉ ra thuật tóan để tìm UCLN đó. Để làm điều này trước hết ta chú ý rằng trong một vành chính D nếu có $a = bq + r$ thì $(a, b) = (b, r)$. Thật vậy, đặt

$$I = <a, b> = \{xa + yb, x, y \in D\} \text{ và } J = < b, r > = \{xb + yr, x, y \in D\}.$$

Từ $a = bq + r$ suy ra $a \in J$, do đó $I \subset J$. Từ $r = a - bq$ suy ra $r \in I$, do đó $J \subset I$. Vậy $I = J$. Như chứng minh trong định lí 6.4 ta có $d = (a, b) = (b, r)$. Bây giờ ta sẽ trình bày thuật tóan tìm ƯCLN cho hai phần tử bất kì trong một vành Euclide .

6.8 Thuật tóan tìm ƯCLN

D là vành Euclide, nên tồn tại ánh xạ $g : D^* \to \angle$ thỏa hai điều kiện trong 6.6. Giả sử $a, b \in D$. Nếu $a, b = 0$ thì $(a,b) = 0$, nếu $a = 0, b \neq 0$ thì $(a, b) = b$. Ta chỉ còn xét cho trường hợp $a, b \neq 0$. Thuật toán là một quá trình thực hiện liên tiếp các phép chia:

. Bước 1: Chia a cho b $a = bq_0 + r_0$, $r_0 = 0$ hoặc $g(r_0) < g(b)$
Nếu $r_0 = 0$ thì dừng. Nếu $r_0 \neq 0$ thì đi đến bước 2

. Bước 2: Chia b cho r_0 $b = r_0q_1 + r_1$, $r_1 = 0$ hoặc $g(r_1) < g(r_0)$
Nếu $r_1 = 0$ thì dừng. Nếu $r_1 \neq 0$, thì đi đến bước 3
. . . . . .

. Bước n : Chia r_{n-1} cho r_n $r_{n-1} = r_n q_{n+1} + r_{n+1}$, $r_{n+1} = 0$ hoặc $g(r_{n+1}) < g(r_n)$

Quá trình chia như vậy phải chấm dứt sau một số hữu hạn bước vì dãy các số tự nhiên $g(b) > g(r_0) > \ldots > g(r_i) > \ldots \geq 0$ không thể giảm vô hạn. Giả sử đến bước n nào đó ta có $r_{n+1} = 0$ và $r_n \neq 0$, thì theo nhận xét ở trên suy ra ƯCLN của a và b là r_n.

6.9 Vành Gauss (Vành nhân tử hóa)

• Một vành nguyên D được gọi là **vành Gauss** hay **vành nhân tử hóa** nếu và chỉ nếu mỗi phần tử p khác 0 và không khả nghịch của nó đều phân tích được thành tích những phần tử bất khả qui

$$p = p_1 p_2 \ldots p_n$$

và sự phân tích này là duy nhất không kể đến thứ tự các nhân tử và các nhân tử sai khác nhau một phần tử khả nghịch.

• CHÚ Ý: Khi phân tích một phần tử p thành tích các nhân tử bất khả qui, một vài hoặc tất cả các nhân tử bất khả qui đó có thể giống nhau. Kết hợp các nhân tử giống nhau lại và biểu diễn tích của chúng dưới dạng lũy thừa thì sẽ dẫn đến dạng sau gọi là **dạng phân tích chính tắc** $p = p_1^{k_1} p_2^{k_2} \ldots . p_m^{k_m}$.

• VÍ DỤ: Vành số nguyên 9 là vành Gauss.

• Một vành nguyên được gọi là thỏa **điều kiện ƯCLN** nếu hai phần tử bất kì của nó đều tồn tại ƯCLN.

• Một vành nguyên D được gọi là thỏa mãn **điều kiện dãy dừng những ước thực sự** nếu mọi dãy $a_1,..., a_n$ ...các phần tử của D sao cho $a_2 \| a_1$, $a_3 \| a_2$,... , $a_n \| a_{n-1}$... đều dừng lại, tức là tồn tại một chỉ số m sao cho $a_m = a_{m+1} = \ldots$

6.10 Định lí

Một miền nguyên là vành Gauss nếu và chỉ nếu nó thỏa mãn điều kiện ƯCLN và điều kiện dãy dừng các ước thực sự .

Chứng minh:
($\Rightarrow$) Giả sử D là vành Gauss.
. Điều kiện ƯCLN: Với mọi a, b $\in D^*$, gọi $\{p_1,...,p_k\}$ là tập hợp tất cả các phần tử bất khả quy khác nhau trong sự phân tích của a và của b. Ta có

$$a \sim p_1^{\alpha_1} \cdots p_k^{\alpha_k} \quad \text{với } \alpha_i \geq 0.$$
$$b \sim p_1^{\beta_1} \cdots p_k^{\beta_k} \quad \text{với } \beta_i \geq 0.$$

Vì mỗi ước của a đều có dạng u. $p_1^{\gamma_1} \cdots p_k^{\gamma_k}$; với $0 \leq \gamma_i \leq \alpha_i$,và mỗi ước của b đều có dạng tương tự với $0 \leq \gamma_j \leq \beta_j$. Nên

$$(a, b) = p_1^{\lambda_1} \cdots p_k^{\lambda_k} \quad \text{với} \quad \lambda_i = \text{Min}(\alpha_i, \beta_i)$$

. Điều kiện dãy dừng các ước thực sự : Giả sử $a \in D$, a khác 0 và không khả nghịch. Đặt l(a) là số các nhân tử trong sự phân tích a thành tích các phần tử bất khả qui. Nếu a = bc, với b và c là những ước thực sự thì ta sẽ được sự phân tích của a thành một tích những phần tử bất khả qui bằng cách nhân các phân tích tương ứng của b và c với nhau. Suy ra rằng l(a) = l(b) + l(c).Vì vậy nếu b || a thì l(b) < l(a). Nếu dãy $a_1,a_2, ..., a_n,...$ các phần tử của D sao cho $a_2 \| a_1$, $a_3 \| a_2$,... , $a_n \| a_{n-1}$... không dừng lại thì ta sẽ có một dãy giảm vô hạn các số nguyên dương $l(a_1) > l(a_2) > ... > l(a_n) > ... \geq 0$, và điều này dẫn đến mâu thuẩn.

($\Leftarrow$) Cho D là miền nguyên thỏa các điều kiện ƯCLN và dãy dừng các ước thực sự.

• Giả sử a là một phần tử của D khác 0 và không khả nghịch. Khi đó a có ít nhất một ước là phần tử bất khả qui, thật vậy
. Nếu a là bất khả qui (đã chứng minh xong).
. Nếu a là khả qui, tức là a có một ước thực sự là a_1.
. Nếu a_1 là bất khả qui (đã chứng minh xong).
. Nếu a_1 là khả qui, tức là a_1 có một ước thực sự là a_2
. . . . . .

Bằng cách lập luận như vậy, sau một số hữu hạn bước, ta sẽ tìm được một ước bất khả qui của a, vì nếu không, thì dãy các ước thực sự $a_1,...,a_n$ ... sẽ không dừng, và điều này mâu thuẫn với giả thiết.

• Theo lí luận trên thì a có ít nhất một ước bất khả qui, giả sử

$$a = p_1 a_1 \quad \text{với } p_1 \text{ bất khả qui}$$

. Nếu a_1 là khả nghịch (sự phân tích đã xong). Nếu a_1 không khả nghịch thì cũng theo trên

$$a_1 = p_2 a_2 \quad \text{với } p_2 \text{ bất khả qui}$$

. Nếu a_2 là khả nghịch (sự phân tích đã xong). Nếu a_2 không khả nghịch thì cũng theo trên $a_2 = p_3 a_3$ với p_3 bất khả qui

. . . . . .

Quá trình này phải chấm dứt sau số hữu hạn bước, vì trong dãy $a_1, a_2, .., a_n, ..$ các phần tử đứng sau là ước thực sự của phần tử đứng liền trước nó. Nếu quá trình dừng sau bước thứ n thì ta có

$$a = p_1 p_2 ... p_n \quad \text{với } p_i \text{ là bất khả qui.}$$

• Giả sử : $p_1 p_2 ... p_n = a = q_1 q_2 ... q_m$, trong đó các p_i, q_j là bất khả qui.
Vì $p_1 \mid q_1 ... q_m$ nên tồn tại $j \in \{1, 2, \ldots, m\}$ sao cho $p_1 \mid q_j$. Bằng cách đánh số lại, ta có thể giả sử $j = 1$, tức là $p_1 \mid q_1$. Vì p_1, q_1 đều bất khả qui nên $p_1 \sim q_1$, suy ra $q_1 = u_1 p_1$ với u_1 khả nghịch. Lúc này ta có

$$p_1 p_2 ... p_n = u_1 p_1 q_2 ... q_m \quad \text{hay} \quad p_2 ... p_n = u_1 q_2 ... q_m ;$$

Bằng lập luận như trên, nếu $n < m$ thì sau n lần giản ước, ta được :

$$1 = u_1 ... u_n q_{n+1} ... q_m$$

nhưng điều này không thể xảy ra vì $q_{n+1}, ..., q_m$, không khả nghịch. Vậy phải có $n \geq m$. Vai trò m, n là như nhau, nên tương tự có $m \geq n$, từ đó $m = n$. Ngòai ra Bằng một cách đánh số thích hợp, ta cũng có $p_i = u_i q_i$ với u_i khả nghịch. □

6.11 Định lí

Mọi vành chính đều là vành Gauss

Chứng minh: Ta đã biết rằng điều kiện ƯCLN được thỏa mãn trên vành chính (định lí 6.4). Do đó, từ định lí 6.10, ta chỉ cần chứng minh điều kiện dãy dừng những ước thực sự cũng được thỏa mãn trên vành chính. Thật vậy, xét dãy các ước thực sự trong vành chính D

$$a_1, a_2, ..., a_n, ... \quad \text{với} \quad a_2 \parallel a_1, a_3 \parallel a_2, ..., a_n \parallel a_{n-1} ...$$

Nếu $a_i \neq a_j$ với mọi $i \neq j$ thì ta có một dãy các ideal

$$< a_1 > \subseteq < a_2 > \subseteq .... \subseteq < a_n > \subseteq$$

Nếu đặt $I = \bigcup_{i=1}^{\infty} < a_i >$ thì I là một ideal của D. Thật vậy, giả sử x, y là hai phần tử bất kì của của I, khi đó tồn tại i, j sao cho $x \in < a_i >$ và $y \in < a_j >$, từ đó x, y $\in < a_k >$ với $k = \max \{i, j\}$. Vì $< a_k >$ là nhóm con nên $x - y \in < a_k >$ và do đó $x - y \in I$. Vậy I là nhóm con của nhóm cộng (D, +). Mặt khác, giả sử x và a là hai phần tử bất kì lần lượt thuộc I và D, khi đó $x \in < a_k >$ với một k nào đó. Vì $< a_k >$ là một ideal nên x a, a x $\in < a_k > \subset$ I. Vậy I là một ideal của D, mà D là vành chính nên I là một ideal chính, tức là $I = < a >$ với $a \in D$. Vì $a \in I$ nên tồn tại n sao cho $a \in < a_n >$, tức là $I \subset < a_n > \subseteq < a_{n+1} > \subset$ I, và điều này dẫn đến mâu thuẫn.

BÀI TẬP

1. Giả sử + và • là hai phép toán trong trên tập $X \neq \emptyset$ thỏa các tính chất

a) (X,+) là nhóm.
b) (X,•) là vị nhóm.
c) Phép toán • phân phối với phép toán +.

Chứng minh rằng (X,+, •) là một vành.

2. Cho 3 là tập các số thực. Trên 3^2 có xác định các phép toán + và • như sau :

$(a, b) + (c, d) = (a + c, b + d)$.
$(a, b) \bullet (c, d) = (ac, ad + bc)$.

Chứng minh rằng $(3^2, +, \bullet)$ là một vành giao hoán.

3. Cho một họ các vành $\{(X_i, +, \bullet), i \in I\}$ và $X = \prod_{i\in I} X_i$. Trên X xác định các phép toán + và • như sau :

$$(x_i)_{i\in I} + (y_i)_{i\in I} = (x_i + y_i)_{i\in I}.$$
$$(x_i)_{i\in I} . (y_i)_{i\in I} = (x_i . y_i)_{i\in I}$$

Chứng minh rằng (X,+, •) là một vành, và X giao hoán nếu các X_i là giao hoán. Vành X được gọi là tích trực tiếp cuả các vành X_i.

4. Đặt 3^3 = {hàm số $f : 3 \to 3$ }. Chứng minh rằng đối với các phép toán cộng và nhân các hàm thông thường thì $(3^3, +, \bullet)$ là một vành giao hóan. 3^3 có phải là một miền nguyên hay không?

5. Ta gọi cấu trúc đại số (X,+, •) là một giả vành nếu các phép toán trong + và • trên X thỏa mãn ba điều kiện sau đây :

a) (X,+) là nhóm giao hoán .
b) (X, •) là nửa nhóm.
c) Phép toán • phân phối với phép toán +.

Chứng minh rằng các tập hợp tương ứng với các phép toán sau là các giả vành

1) Tập hợp các hàm số thực liên tục f trên 3 sao cho : $\int_{-\infty}^{+\infty} |f(x)|dx < \infty$

với các phép toán cộng và nhân thông thường các hàm.
2) Tập hợp 29 với phép toán cộng và nhân các số.
3) X = { 0, a, b, c } với các phép toán trên X được cho bởi

+	0	a	b	C

•	0	a	b	c

0	0	a	b	c
a	a	0	c	b
b	b	c	0	a
c	c	b	a	0

0	0	0	0	0
a	0	a	b	c
b	0	0	0	0
c	0	a	b	c

4) Tập $X = \{(a, b, -b, a) : a, b \in 9\}$, với các phép toán + và • như sau :

$(a, b, -b, a) + (c, d, -d, c) = (a + c, b + d, -b - d, a + c)$
$(a, b, -b, a) \bullet (c, d, -d, c) = (ac - bd, ad + bc, -ad - bc, ac - bd)$.

6. Cho $(X,+, \bullet)$ là một giả vành và $Z(X) = \{x \in X : ax = xa, \text{với mọi } a \in X\}$ là tâm của X. Giả sử với mọi $x \in X$, $x^2 - x \in Z(X)$.
a) Chứng minh rằng với mọi $x, y \in X$, $xy + yx \in Z(X)$.
b) Suy ra $xy = yx$ với mọi $x, y \in X$.

7. Trong một vành giao hoán X, hãy chứng minh công thức nhị thức Newton

$$(a+b)^n = \sum_{k=0}^{n} C_n^k a^k b^{n-k}$$

8. Đối với các phép toán cộng và nhân các hàm số thông thường chứng tỏ tập $3^{[0,1]} = \{\text{hàm số } f : [0, 1] \to 3\}$ là một vành giao hoán. Các tập hợp sau có phải là vành con của $3^{[0,1]}$
a) Tập hợp các hàm số liên tục trên [0,1].
b) Tập hợp các hàm số khả tích trên [0,1].

9. Chứng minh rằng

a) $9[i] = \{ a + bi : a, b \in 9\}$ là vành con của $(\forall,+, \bullet)$.
b) $9[\sqrt{2}] = \{ a + b\sqrt{2} : a, b \in 9\}$ là vành con của $(3,+, \bullet)$.
c) $\Theta[\sqrt{2}] = \{ a + b\sqrt{2} : a,b \in \Theta\}$ là trường con của $(R,+, \cdot)$

10. Cho một họ các vành con $\{A_i, i \in I\}$ của X. Giả sử rằng, với mọi $i, j \in I$ tồn tại $k \in I$ sao cho A_i và A_j đều chứa trong A_k . Chứng minh rằng $\bigcup_{i \in I} A_i$ là vành con của X.

11. Cho $(X,+, \bullet)$ là một vành và gọi $Z(X) = \{a \in X : ax = xa, \text{với mọi } x \in X\}$ là tâm của X. Chứng minh rằng Z(X) là vành con của X.

12. Cho $(X,+, \bullet)$ là một vành và $A = \{a \in X : \text{tồn tại } n \in \angle : a^n = 0\}$. A có phải là vành con của X không?

13. Cho $(X,+, \bullet)$ là một vành và $f : X \to X$ là một đồng cấu vành. Chứng minh rằng $A = \{ a \in X : f(x) = x \}$ là vành con của X.

14. Tìm tất cả các tự đồng cấu vành của các vành 9, 9 [$\sqrt{2}$], 9 [i].

15. Cho Θ là tập các số hữu tỉ. Trên Θ^2 xác định các phép toán + và • như sau :

(a, b) + (c, d) = (a + c, b + d) .

(a, b) • (c, d) = (ac + 2bd, ad + bc) .

Chứng minh rằng (Θ^2,+, •) là một vành và nó đẳng cấu với (Θ [$\sqrt{2}$],+, •) .

16. Cho (X,+,•) là một vành và End(X) là vành các tự đồng cấu của nhóm cộng (X,+). Với mỗi a ∈ X, định nghĩa ánh xạ : f_a : X → X , f_a (x) = ax.

a) Chứng minh rằng f_a ∈ End(X).

b) .Chứng minh rằng ánh xạ h : X → End(X) , a ↦ f_a , là đơn cấu vành.

Suy ra rằng mọi vành có thể xem như là vành con của vành các tự đồng cấu của nhóm cộng của nó.

17. Cho một vành X. .Chứng minh rằng tồn tại duy nhất một đồng cấu vành f :9 → X. Hơn nữa, nếu X có đặc số 0 thì f là đơn cấu.

18. Chứng minh rằng các vành sau đây có đặc số 0 : 9, Θ , 3, ∀ , Mat_3 (n), End(9).

19. Chứng minh rằng mọi vành hữu hạn có đặc số m > 0.

20. Cho (X,+, •) là một một vành và n∈9. Chứng tỏ A = { x ∈ X : nx = 0} là ideal của X.

21. Cho (X,+, •) là một vành giao hoán. . Chứng minh rằng tập con A = { x ∈ X : rx = 0 ; với mọi r ∈ X } là ideal của X.

22. Cho (X,+, •) là một vành giao hoán và A, B là các ideal của X. Chứng minh rằng C = {x∈ X : x b ∈ A , với mọi b ∈ B} là một ideal của X.

23. Cho A là tập con khác rỗng của vành X. . Chứng minh rằng tập con

$$(A) = \left\{ \sum_{i=1}^{n} x_i a_i y_i \ : \ x_i, y_i \in X; \ a_i \in A; \ i \in \overline{1,n}; \ n \in N \right\}.$$

là một ideal của X

24. Cho A là ideal và B là vành con của vành X. Chứng minh rằng

a) A + B là một vành con của X.

b) A ∩ B là ideal của B.

c) A là một ideal của A + B.

d) $B/(A \cap B)$ đẳng cấu với $(A + B)/A$.

25. Cho X_1, X_2 là hai vành và $A_1 = X_1 \times \{0\}$, $A_2 = \{0\} \times X_2$.

a) Chứng minh rằng A_1, A_2 là các ideal của vành tích $X = X_1 \times X_2$ thỏa :
$A_1 \cap A_2 = \{0\}$ và $A_1 + A_2 = X$.

b) Chứng tỏ phép chiếu $p_i : X \to X_i$, $(x_1, x_2) \mapsto x_i$ là một toàn cấu. Xác định $Kerp_i$. Chứng minh rằng $X/A_j \cong X_i$ với $i,j \in \{1, 2\}$ và $i \neq j$.

c) Chứng tỏ A_1, A_2 là các vành đối với các phép toán + và $\bullet$ xác định trên X, nhưng không phải là vành con của X.

26. Vành nào trong các vành sau là miền nguyên, trường : $9_3, 9_4, 9_5, 9_6, 9_{48}$, X^A = {ánh xạ $f : A \to X$}

27. Chứng minh rằng $\Theta[\sqrt{2}]$ là trường. $9[\sqrt{2}]$ có phải là trường không ?

28. Trong Θ , cho các phép toán :

$$a * b = a + b - 1 \quad \text{và} \quad a \perp b = a + b - ab.$$

$(\Theta, *, \perp)$ có phải là một trường không?

29. Cho T là tập các ma trận dạng $\begin{pmatrix} a & b \\ 2b & a \end{pmatrix}$ trong đó $a, b \in \Theta$. Chứng minh rằng đối với phép cộng và nhân ma trận, T là một trường và T đẳng cấu với trường $\Theta[\sqrt{2}]$.

30. Chứng minh rằng vành con của miền nguyên là miền nguyên.

31. Chứng minh rằng mọi trường hữu hạn đều có đặc số khác 0. Mọi trường đều có đặc số 0 hay là số nguyên tố.

32. Nếu $(X,+,\cdot)$ là một trường có đặc số p. Chứng minh rằng

a) $(x + y)^p = x^p + y^p$.
b) $(x - y)^p = x^p - y^p$.

33. Trong vành giao hoán X, một phần tử x được gọi là lũy linh nếu tồn tại $n \in \angle$ sao cho $x^n = 0$. Chứng minh rằng
a) Nếu x, y là lũy linh thì x + y cũng lũy linh.
b) Nếu x lũy linh thì $(1 + x) \mid 1$.

c) Nếu x lũy linh và u | 1 thì (u + x) | 1.

34.

a) Chỉ ra rằng $A = \{a + b\sqrt{-3}, a, b \in 9\} \subset \forall$ là một vành nguyên.

b) Chứng minh rằng phần tử 2, $1 + \sqrt{-3}$, $1 - \sqrt{-3}$, là những phần tử bất khả qui. Chứng tỏ phần tử 4 có hai dạng phân tích thành nhân tử bất khả qui khác nhau. Từ đó suy ra A không phải là một vành chính.

35. Chứng minh rằng mọi trường đều là vành chính.

36.

a) Vành con của một vành chính có phải là vành chính không?

b) Vành thương của một vành chính có phải là một vành chính hay không?

37. Cho A là một vành chính và p là một phần tử bất khả qui của A. Chứng minh rằng vành thương $A/_{<p>}$ là một trường.

38. Một vành A được gọi là vành Boole nếu và chỉ nếu $x^2 = x$ với mọi $x \in A$. Cho một tập E. Chứng minh rằng

a) $((9_2)^E, +, \bullet)$ là một vành Boole, trong đó 9_2 là vành các số nguyên modulo 2 và $(9_2)^E$ là tập các ánh xạ từ E đến 9_2.

b) (P(E), Δ, $\cap$) là một vành Boole, trong đó P(E) là tập các tập con của E và Δ là hiệu đối xứng

c) Cho A là một tập con của E, ta kí hiệu $\chi_A(x) : E \to 9_2$, được xác định bởi

$$\chi_A(x) = \begin{cases} \bar{1} \text{ khi } x \in A \\ \bar{0} \text{ khi } x \notin A \end{cases}$$

gọi là hàm đặc trưng của A. Khi đó ánh xạ $P(E) \to (9_2)^E$, $A \mapsto \chi_A$, là một đẳng cấu vành.

CHƯƠNG 5:
VÀNH ĐA THỨC

1 Vành đa thức một biến

1.1 Định nghĩa

• Giả sử A là một vành giao hóan với phần tử đơn vị là $1 \neq 0$. Gọi M là tập hợp các dãy $(a_1. a_2, \ldots,a_n,\ldots)$ trong đó các $a_i \in A$ và chỉ có một số hữu hạn trong chúng là khác 0. Trên M xác định một phép tóan cộng và một phép tóan nhân như sau :

$$(a_0, a_1, \ldots,a_n\ldots) + (b_0, b_1, \ldots,b_n\ldots) = (a_0 + b_0, a_1 + b_1, \ldots,a_n + b_n,\ldots)$$

$$(a_0. a_1, \ldots,a_n\ldots).(b_0. b_1, \ldots,b_n\ldots) = (c_0, c_1 , \ldots,c_n,\ldots),$$

trong đó $$c_k = \sum_{i+j=k} a_i b_j \text{ , } k = 0, 1, 2,\ldots.$$

• Khi đó (M, +) là một nhóm giao hóan với phần tử đơn vị $0 = (0, 0, \ldots,0,\ldots)$, phần tử nghịch đảo của phần tử $(a_0, a_1, \ldots,a_n\ldots)$ là $(-a_0, -a_1, \ldots,-a_n\ldots)$ và (M, •) là một vị nhóm giao hóan với phần tử đơn vị là $(1, 0, \ldots,0,\ldots)$. Ngòai ra phép tóan • cũng phân phối đối với phép toán + nhờ đẳng thức :

$$\sum_{i+j=k} a_i(b_j + c_j) = \sum_{i+j=k} a_i b_j + \sum_{i+j=k} a_i c_j .$$

Từ đó (M, +, •) là một vành giao hoán.

• Nếu đặt $M' = \{(a, 0,\ldots,0,..), a \in A \} \subset M$, thì (M',+, •) là một vành con của M và từ đẳng cấu vành $f : A \xrightarrow{\cong} M', a \mapsto (a,0,\ldots,0,..)$, ta có thể đồng nhất một phần tử $a \in A$ với dãy $(a, 0, \ldots,0,\ldots) \in M$. Vì vậy A cũng được xem như một vành con của M.

• Nếu ta ký hiệu $x = (0, 1, 0,\ldots,0,\ldots)$ thì từ định nghĩa phép tóan • và + ta được :

$$x^2 = (0, 0, 1, 0, 0,\ldots,0,\ldots)$$
$$x^3 = (0, 0, 0, 1, 0,\ldots,0,\ldots)$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$x^n = (0,0,\ldots,0, 1, 0,\ldots,0\ldots)$$

Ta qui ước viết $x^0 = (1, 0,0,\ldots,0,\ldots) = 1$

• Vì chỉ có một số hữu hạn các phần tử a_i trong dãy $(a_0, a_1, \ldots,a_n\ldots)$ là khác 0 nên ta có thể qui ước viết mỗi phần tử khác 0 của M dưới dạng

$(a_0, a_1, \ldots, a_n, 0, \ldots)$, trong đó $a_n \neq 0$ và $a_m = 0$ với mọi $m > n$

Theo qui ước cách viết đó, và từ định nghĩa phép tóan $\bullet$ và + trên M, mỗi phần tử $(a_0, a_1, \ldots, a_n, 0, \ldots) \in M$ có thể biểu diễn dưới dạng :

$(a_0, a_1, \ldots, a_n, 0, ..) = (a_0, 0, \ldots.) + (a_1, 0, \ldots.).(0,1,0, \ldots) + \ldots + (a_n, 0, \ldots).(0, \ldots, 0,1,0, ..)$

$$= a_0 + a_1 x + \ldots. + a_n x^n = \sum_{i=0}^{n} a_i x^i = f(x)$$

- Vành $(M,+,\bullet)$ được gọi là **vành đa thức của biến** x trên A, kí hiệu là A[x].

Các phần tử $f(x) = \sum_{i=0}^{n} a_i x^i \in A[x]$ được gọi là một **đa thức của biến x.** Các a_i gọi là các **hệ tử của đa thức**. Các $a_i x^i$ gọi là các **hạng tử của đa thức**, đặc biệt $a_0 x^0 = a_0$ gọi là **hạng tử tự do**. Nếu $a_n \neq 0$ thì số n được gọi là **bậc của đa thức f**, và kí hiệu deg(f) = n, còn a_n được gọi là **hệ tử cao nhất của đa thức** f(x). Đa thức với các hệ tử đều bằng 0 gọi là **đa thức không.** Đa thức bậc 0 là một phần tử của vành A và nó còn được gọi là **đa thức hằng**. Chú ý rằng ta không định nghĩa bậc của đa thức 0.

1.2 Định lí

Cho f(x) và g(x) là hai đa thức . Khi đó :

1) Nếu $f(x) + g(x) \neq 0$ thì $\deg(f + g) \leq \max\{\deg(f), \deg(g)\}$. Hơn nữa nếu giả thiết thêm deg(f) = deg(g) thì $\deg(f + g) = \deg(f) = \deg(g)$

2) Nếu $f(x)g(x) \neq 0$ thì $\deg(f.g) \leq \deg(f) + \deg(g)$. Hơn nữa nếu giả thiết thêm A là vành nguyên thì $\deg(f.g) = \deg(f) + \deg(g)$.

Chứng minh: Giả sử $f = \sum_{i=0}^{n} a_i x^i$, $g = \sum_{i=0}^{m} b_i x^i$, với $a_n, b_m \neq 0$, $m = n + k$, $k \geq 0$.

Khi đó $f + g = \sum_{i=0}^{n} (a_i + b_i) x^i + \sum_{i=n+1}^{m} b_i x^i$

và $f.g = a_0 b_0 + \ldots + (a_0 b_k + a_1 b_{k-1} + \ldots a_k b_0) x^k + \ldots + a_n b_m x^{n+m}$

Chú ý rằng, nếu A là vành nguyên thì $a_n b_m \neq 0$. Từ đó, suy ra các khẳng định đã nêu trong định lí. □

1.3 Định lí

Nếu A là một vành nguyên thì A[x] cũng là một vành nguyên.

Chứng minh : Giả sử $f = \sum_{i=0}^{n} a_i x^i$, $g = \sum_{i=0}^{m} b_i x^i$ (với $a_n, b_m \neq 0$) là hai đa thức khác không bất kì. Khi đó $f.g = a_0b_0 + \ldots + (a_0b_k + \ldots + a_kb_0)\, x^k + \ldots + a_n b_m x^{n+m}$.

Vì trong A không có ước của 0 nên từ $a_n, b_m \neq 0$ suy ra $a_nb_m \neq 0$, do đó $f.g \neq 0$ □

1.4 Định lí

Nếu K là một trường thì vành K[x] là vành Euclide, và do đó nó cũng là vành chính, vành Gauss.

Chứng minh :

Từ 1.3 suy ra K[x] là một vành nguyên. Xét ánh xạ

$$\deg : K[x] - \{0\} \to \angle,\ f \mapsto \deg(f).$$

Từ 1.2 suy ra $\deg(fg) = \deg(f) + \deg(g) \geq \deg(f)$.

Bây giờ, với mọi $f, g \in K[x]$ và $g \neq 0$, ta sẽ chỉ ra tồn tại duy nhất $q, r \in K[x]$ sao cho $f = qg + r$ với $r = 0$ hoặc $\deg(r) < \deg(g)$.

. *Tồn tại*.
Nếu $f = 0$ thì ta lấy $q = 0, r = 0$. Nếu với $f \neq 0$ và $\deg(f) < \deg(g)$ thì ta lấy $q = 0$, $r = f$. Vậy chỉ cần xét trường hợp $f \neq 0$ và $\deg(f) \geq \deg(g)$). Ta chứng minh bằng cách qui nạp theo deg(f).

- Với $\deg(f) = 0$, khi đó $\deg(g) = 0$, tức là $f, g \in K, g \neq 0$, từ đó chỉ cần chọn $q = f.g^{-1}$ và $r = 0$.

- Giả sử khẳng định đúng cho các đa thức với bậc $< \deg(f)$, ta chỉ ra khẳng định đúng cho deg(f). Nếu $f = \sum_{i=0}^{n} a_i x^i$, $g = \sum_{i=0}^{m} b_i x^i$ thì đặt $f_1 = f - b_m^{-1} a_n x^{n-m} g$. Khi đó $f_1 = 0$ hoặc $\deg(f_1) < \deg(f)$. Nếu $f_1 = 0$ thì khẳng định đã được chứng minh.
Nếu $\deg(f_1) < \deg(f)$ thì theo giả thiết qui nạp tồn tại $q_1, r_1 \in K[x]$ sao cho $f_1 = q_1 . g + r_1$, với $r_1 = 0$ hoặc $\deg(r_1) < \deg(g)$. Từ đó
$f = f_1 + b_m^{-1} a_n x^{n-m} g = q_1 g + r_1 + b_m^{-1} a_n x^{n-m} g = (q_1 + b_m^{-1} a_n x^{n-m})g + r_1$.

. *Duy nhất* . Giả sử có $f = qg + r = q'g + r'$. Khi đó $(q - q')g = r - r'$. Nếu $r \neq r'$ thì $(q - q')g \neq 0$, suy ra $\deg(r - r') = \deg(q - q') + \deg(g)$ (mâu thuẩn vì khi đó $\deg(g) \leq \deg(r - r') \leq \max\{\deg(r), \deg(r')\} < \deg(g)$).Vậy $r = r'$ và từ đó $q = q'$. □

• VÍ DỤ:

1) Thực hiện phép chia Euclide đa thức $f = x^5 + x^2 + 1$ cho $g = x^3 + 3x^2 - 4$ trên vành $\mathbb{Z}[x]$.

$$\begin{array}{l|l}
x^5 + 0x^4 + 0x^3 + x^2 + 0x + 1 & x^3 + 3x^2 - 4 \\
\underline{x^5 + 3x^4 + \quad\quad - 4x^2 \quad\quad\quad .} & \hline \\
-3x^4 + \quad + 5x^2 \quad\quad + 1 & x^2 - 3x + 9 \\
\underline{-3x^4 - 9x^3 \quad\quad + 12x + 1} & \\
9x^3 + 5x^2 - 12x + 1 & \\
\underline{9x^3 + 27x^2 \quad\quad - 36} & \\
-22x^2 - 12x + 37 &
\end{array}$$

Từ đó $x^5 + x^2 + 1 = (x^3 + 3x^2 - 4)(x^2 - 3x + 9) - 22x^2 - 12x + 37$

2) Thực hiện phép chia đa thức $f = \bar{1}x^5 + \bar{1}x^2 + \bar{1}$ cho $g = \bar{1}x^3 + \bar{3}x^2 - \bar{4}$ trên vành $\mathbb{Z}_5[x]$.

$$\begin{array}{l|l}
\bar{1}x^5 + \bar{0}x^4 + \bar{0}x^3 + \bar{1}x^2 + \bar{0}x + \bar{1} & \bar{1}x^3 + \bar{3}x^2 - \bar{4} \\
\bar{1}x^5 + \bar{3}x^4 \quad\quad - \bar{4}x^2 & \hline \\
\hline & \bar{1}x^2 - \bar{3}x + \bar{4} \\
-\bar{3}x^4 \quad\quad\quad + \bar{1} & \\
-\bar{3}x^4 - \bar{4}x^3 \quad + \bar{2}x & \\
\hline & \\
\bar{4}x^3 \quad - \bar{2}x + \bar{1} & \\
\bar{4}x^3 + \bar{2}x^2 \quad - \bar{1} & \\
\hline & \\
-\bar{2}x^2 - \bar{2}x + \bar{2} &
\end{array}$$

Từ đó, $\bar{1}x^5 + \bar{1}x^2 + \bar{1} = (\bar{1}x^3 + \bar{3}x^2 - \bar{4})(\bar{1}x^2 - \bar{3}x + \bar{4}) - \bar{2}x^2 - \bar{2}x + \bar{2}$

1.5 Không điểm của đa thức

- Cho vành A , c là một phần tử của A và $f(x) = \sum_{i=0}^{n} a_i x^i$ là một đa thức của A[x] . Phần tử $f(c) := \sum_{i=0}^{n} a_i c^i$ sẽ được gọi là **giá trị của đa thức f(x) tại c**. Nếu f(c) = 0 thì ta nói c là một **không điểm** hay là **nghiệm** của f(x). Việc tìm tất cả các nghiệm của f(x) trong A được gọi là **giải phương trình đại số bậc n** $\sum_{i=0}^{n} a_i x^i = 0$ trong A.

1.6 Định lí

Giả sử K là một trường, c là một phần tử của A và $f(x) = \sum_{i=0}^{n} a_i x^i$ là một đa thức của K[x]. Khi đó c là một nghiệm của f(x) khi và chỉ khi $(x - c) \mid f(x)$

Chứng minh : Thực hiện phép chia Euclide $f(x) = (x – c)g(x) + r$. Từ đó suy ra $r = f(c)$. Vậy có thể viết $f(x) = (x – c)g(x) + f(c)$. Khi đó khẳng định là rõ ràng. □

1.7 Cấp của không điểm

Cho K là một trường, $c \in K$, $f(x) \in K[x]$ và $m \geq 1$ là một số tự nhiên. Ta nói c là **nghiệm bội cấp m** của f(x) nếu chia hết cho $(x – c)^m$ và không chia hết cho $(x – c)^{m+1}$. Nếu m = 1 ta còn nói c là **nghiệm đơn**, nếu m = 2 thì c được gọi là **nghiệm kép**. Ta cũng có thể xem một đa thức có một nghiệm bội cấp m như một đa thức có m nghiệm trùng nhau.

1.8 Định lí

Giả sử K là một trường sao cho mọi đa thức khác hằng trong K[x] đều có nghiệm trong K. Khi đó với mọi đa thức $f \in K[x]$ tồn tại các phần tử $a_1, a_2, \ldots, a_n \in K$ và $c \in K$ sao cho $f(x) = c(x – a_1)(x – a_2) \ldots (x – a_n)$.

Chứng minh : Giả sử a_1 là một nghiệm của đa thức f(x). Theo định lí 1.6 ta có $f(x) = (x – a_1)q(x)$ với $\deg(q) = \deg(f) – 1$. Nếu q là khác hằng thì theo giả thiết tìm được một nghiệm của q(x) là a_2 và như thế ta có

$$f(x) = q_1(x)(x – a_1)(x – a_2)$$

Tiếp tục lí luận như trên cho đến khi q_n là hằng thì ta sẽ có điều cần chứng minh. □

• Một trường K có tính chất như định lí 1.8, đó là mọi đa thức khác hằng trên K đều có một nghiệm trên K, được gọi là **trường đóng đại số**. Cho dù K không đóng đại số ta cũng có:

1.9 Định lí

Mọi đa thức bậc $n \geq 1$ trên một trường K có nhiều nhất là n nghiệm kể cả bội.

Chứng minh : Giả sử đa thức f(x) có k nghiệm phân biệt $a_1, a_2, \ldots, a_k$ với bội tương ứng là $m_1, m_2, \ldots, m_k$ thì bởi phép chia Euclide ta có phân tích

$$f(x) = (x – a_1)^{m_1} (x – a_2)^{m_2} \ldots (x – a_n)^{m_k} q(x)$$

Từ đó suy ra $m_1 + m_2 + \ldots + m_k \leq \deg(f) = n$. □

1.10 Định lí

Cho K là một trường vô hạn, và $f(x) = \sum_{i=0}^{n} a_i x^i$, $g(x) = \sum_{i=0}^{n} b_i x^i$ là hai đa thức trong K[x]. Khi đó nếu f(c) = g(c) với mọi $c \in K$ thì f = g, tức là $a_k = b_k$ với mọi k = 0, 1, …, n.

Chứng minh : Xét đa thức $f(x) - g(x) = \sum_{i=0}^{n} (a_i - b_i)x^i$, khi đó theo giả thiết mỗi phần tử của K là một nghiệm của đa thức này. Từ đó, bởi định lí 1.9, phải có $a_k = b_k$ với mọi k = 0, 1, …, n. □

1.11 Hàm đa thức

• Với mọi đa thức $f(x) = \sum_{i=0}^{n} a_i x^i \in K[x]$ ta xác định một ánh xạ như sau

$$\hat{f} : K \to K,\ \hat{f}(c) = \sum_{i=0}^{n} a_i c^i$$

và gọi là **hàm đa thức tương ứng với f.**

• CHÚ Ý: Xét ánh xạ $\varphi : K[x] \to K^K = \{\text{ánh xạ: } K \to K\}$, $f \mapsto \hat{f}$, và có thể kiểm tra dễ dàng rằng đó là một đồng cấu vành. Ta sẽ khảo sát tính đơn ánh của φ.

a) Giả sử $K = \{t_1, t_2, \ldots, t_N\}$ hữu hạn và xét $f = \prod_{k=1}^{N} (x - t_k) \in K[x]$. Khi đó ta có $f \neq 0$ vì $\deg(f) = N \geq 1$ nhưng rõ ràng $\hat{f} = 0$ vì $\hat{f}(c) = 0$ với mọi $c \in K$. Như vậy ta có $f \neq 0$ mà $\varphi(f) = \varphi(0) = 0$. Từ đó φ là không đơn ánh.

b) Giả sử K vô hạn. Khi đó φ là đơn ánh vì từ $\varphi(f) = \varphi(g)$ suy ra $\hat{f}(c) = \hat{g}(c)$ với mọi $c \in K$, hay f(c) = g(c) với mọi $c \in K$, và theo định lí 1.10, f = g.

Như vậy φ là một đơn cấu vành khi và chỉ khi trường K là vô hạn. Từ đó, nếu K là vô hạn (Chẳng hạn 3 và $\forall$) thì ta có thể đồng nhất f với $\hat{f}$, tức là xem đa thức f như là một hàm xác định trên K.

• Bây giờ ta sử dụng các kết qủa đã thu được về vành chính và vành Euclide để nghiên cứu vành đa thức K[x] với K là một trường. Trước hết chú ý rằng :

1) Phần tử khả nghịch trong K[x] là các phần tử $a \in K^* = K - \{0\}$.

2) Đa thức liên kết với đa thức f(x) là các đa thức có dạng af(x) với $a \in K^*$.

3) Phần tử bất khả qui trong K[x] là các đa thức p(x) có bậc ≥ 1, mà ước của nó chỉ có thể là các đa thức hằng (các phần tử thuộc K^*) và các đa thức có dạng c p(x) với $c \in K^*$. Rõ ràng các đa thức bậc 1 : ax + b là bất khả qui . Chúng có nghiệm là $-a^{-1}b$ trong K. Các đa thức bất khả qui khác tức là các đa thức bất khả qui có bậc > 1 là vô nghiệm trong K. Thật vậy, nếu p(x) là một đa thức bất khả qui có bậc > 1 và có nghiệm $c \in K$ thì

$$p(x) = (x - c).q(x) \text{ với } \deg(q) \geq 1.$$

Do đó (x – c) là ước thực sự của p(x), điều này trái với p(x) là bất khả qui.

1.12 Định lí

Cho K là một trường và $p(x) = \sum_{i=0}^{n} a_i x^i$ (n >1) là một đa thức bất khả qui trên vành K [x]. Khi đó tồn tại một trường T duy nhất (theo nghĩa sai khác nhau một đẳng cấu) sao cho :

1) K là một trường con của T.
2) p(x) có một nghiệm u trong T
3) Mọi phần tử $z \in T$ đều viết được duy nhất dưới dạng $z = \sum_{i=0}^{n-1} b_i u^i$, $b_i \in K$.

Chứng minh :

. Đặt $I = < p(x) >$ là ideal sinh bởi p(x) , và xét vành thương $T = K[x]/ I$. Khi đó T cũng là một trường. Thật vậy, xét $f(x) + I \neq 0 + I$, khi đó vì f(x) không phải là bội của p(x) nên (f(x), p(x)) = 1. Từ đó tồn tại r(x), s(x) $\in$ K[x] sao cho f.r + p.s = 1, suy ra $f.r \in 1 + I$. Vậy ta có

$$(f(x) + I).(r(x) + I) = f(x).r(x) + I = 1 + I.$$

tức là f(x) + I khả nghịch.

. Bây giờ xét tòan cấu chính tắc $\pi : K[x] \to K[x] / I$, $f \mapsto f + I$, và thu hẹp của nó trên K $\pi|_K : K \to K [x] / I$, và ta có thể dễ kiểm tra $\pi|_K$ là một đơn cấu. Từ đó có thể đồng nhất các phần tử $a \in K$ với $\pi|_K (a) \in K [x] / I = T$ và xem K là một trường con của T. Nếu đặt $u = \pi (x)$, thì ta có thể viết

$$\pi(p(x)) = \sum_{i=0}^{n} \pi(a_i)\pi(x)^i = \sum_{i=0}^{n} a_i u^i .$$

Vì $\pi(p(x)) = p(x) + I = 0 + I$ nên ta có $\sum_{i=0}^{n} a_i u^i = 0 + I$ (phần tử không trong T), điều này có nghĩa là u là nghiệm trong T của đa thức p(x).

. Cuối cùng lấy z bất kì thuộc T, khi đó tồn tại $f \in K[x]$ sao cho $z = \pi(f)$. Chia f cho p(x) ta được

$f(x) = p(x)\, g(x) + r(x)$, với $r(x) = \sum_{i=0}^{n-1} b_i x^i$ ($b_i \in K$ và không nhất thiết $\neq 0$). Từ đó $z = \pi(f) = \pi(p.g) + \pi(r) = 0 + \pi(r) = \sum_{i=0}^{n-1} b_i u^i$.

Biểu diễn của z là duy nhất . Thật vậy

Giả sử $z = \sum_{i=0}^{n-1} b_i u^i = \sum_{i=0}^{n-1} c_i u^i$. Khi đó : $\sum_{i=0}^{n-1} (b_i - c_i)u^i = \pi(\sum_{i=0}^{n-1} (b_i - c_i)x^i) = 0$,

tức là $\sum_{i=0}^{n-1} (b_i - c_i)x^i \in I$, suy ra $\sum_{i=0}^{n-1} (b_i - c_i)x^i$ là bội của p(x), điều này chỉ xảy ra khi $b_i = c_i$ (do bậc của p(x) lớn hơn).

. Bây giờ ta chỉ ra T là duy nhất sai khác một đẳng cấu. Giả sử có một trường T' cũng có các tính chất như T. Gọi u' là nghiệm của p(x) trong T'. Xét đồng cấu $\varphi : K[x] \to T'$, $f(x) \mapsto f(u')$. Có thể chỉ ra φ là tòan cấu và $\mathrm{Ker}\,\varphi = I$. Từ đó theo định lí đồng cấu vành : $T' = \mathrm{Im}\,\varphi \cong K[x]/\mathrm{Ker}\,\varphi = K[x]/I = T$. □

• ÁP DỤNG : Áp dụng định lí 1.12 cho trường hợp K = 3 là tập các số thực và $p(x) = x^2 + 1$ thì trường T lúc nãy sẽ là

$$^{3[x]}/_{<x^2+1>} = \{a + b.i;\ a,b \in 3 \text{ và } i \text{ là nghiệm của } x^2 + 1 = 0\} = \forall .$$

Như vậy ta tìm lại được trường số phức quen thuộc.

1.13 Định lí

Cho K là một trường, $f(x) \in K[x]$ là đa thức có bậc $n > 1$. Khi đó tồn tại một trường T mở rộng của K sao cho f(x) có đúng n nghiệm.

Chứng minh : Nếu các nhân tử bất khả qui trong phân tích của f đều là bậc 1 thì đã chứng minh xong. Giả sử có p(x) là một nhân tử bất khả qui với bậc > 1. Ta xây dựng trường T để p(x) có nghiệm trong T. Nếu f(x) chưa có n nghiệm thì nó phải có dạng :

$$f(x) = (x-a)^r.....(x-b)^s.f_1(x),$$

trong đó $a,\ldots,b \in T$ và $f_1(x) \in T[x]$, $1 < \deg(f_1) < \deg(f)$

Tiếp tục mở rộng trường T thành T_1 để $f_1(x)$ có nghiệm trong T_1. Vì bậc của đa thức là hữu hạn nên sau một số hữu hạn bước ta sẽ tìm được trường mở rộng T_k thỏa yêu cầu . □

2. Vành đa thức nhiều biến

2.1 Định nghĩa

• Giả sử A là một vành giao hóan với đơn vị 1. Ta đặt :

$$A_1 = A[x_1], A_2 = A_1[x_2], \ldots, A_n = A_{n-1}[x_n].$$

Khi đó vành $A_n = A_{n-1}[x_n]$, được kí hiệu là $A[x_1, x_2, \ldots,x_n]$, sẽ được gọi là **vành đa thức của n biến** trên A. Mỗi phần tử của $A[x_1, x_2, \ldots,x_n]$ được gọi là một đa thức của n biến $x_1, x_2, \ldots,x_n$, và viết $f(x_1, x_2, \ldots,x_n) \in A[x_1, x_2, \ldots,x_n]$.

Bây giờ ta tìm cách biểu diễn các phần tử của vành $A[x_1, x_2, \ldots,x_n]$.
Trước hết xét các đa thức hai biến $f(x,y) \in A[x,y] = A[x][y]$. Nó có thể viết dưới dạng :

$$f(x,y) = a_0(x) + a_1(x)y + ...+ a_n(x)y^n$$

với $$a_i(x) = \sum_{k=0}^{m_i} b_{ik}x^k \in A[x]$$

Vì A [x, y] là vành nên phép nhân phân phối đối với phép cộng , do đó f(x,y) có thể viết

$$f(x,y) = \sum c_{m_i m_j} x^{m_i} y^{m_j}, \quad \text{với } c_{m_i m_j} \in A.$$

Bằng qui nạp ta thấy đa thức biến có thể viết dưới dạng :

$$f(x_1, x_2, \ldots,x_n) = \sum c_{m_i.....m_n} x_1^{m_i} .....x_n^{m_n}, \text{ với } c_{m_i...m_n} \in A, \quad (1)$$

Mỗi hạng tử $g = ax_1^{m_1} \ldots x_n^{m_n}$ với $a \in A$ gọi là môt **đơn thức**, nếu $a \neq 0$ thì tổng $m_1 + m_2 + \ldots + m_n$ được gọi là **bậc của đơn thức g**, và kí hiệu là deg(g). Ta định nghĩa **bậc của một đa thức f** bất kì viết dưới dạng (1) là

$$\deg(f) = \max \{ m_1 + m_2 + \ldots + m_n : c_{m_i...m_n} \neq 0\}$$

2.2 Cách sắp xếp đa thức theo lối tự điển

• Xét vị nhóm cộng giao hoán $\angle_0^n = \angle_0 \times \angle_0 \times \ldots \times \angle_0$ với phép cộng được xác định bởi $(a_1, a_2, \ldots, a_n) + (b_1, b_2, \ldots, b_n) = (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n)$. Trên $\angle_0^n$ xác định một quan hệ $>$ như sau : $(a_1, a_2, \ldots, a_n) > (b_1, b_2, \ldots, b_n)$ nếu và chỉ nếu tồn tại $i \in \{1, 2, \ldots, n\}$ sao cho

$$a_1 = b_1, a_2 = b_2, \ldots, a_{i-1} = b_{i-1} \text{ và } a_i > b_i .$$

VÍ DỤ: Trên $\angle_0^3$, $(2, 1, 1) > (1, 2, 3) > (0, 4, 1) > (0, 3, 9)$

Có thể kiểm tra dễ dàng rằng $(\angle_0^n, >)$ là một vị nhóm được sắp thứ tự tòan phần.

• Sắp xếp đa thức $f(x_1, x_2, \ldots, x_n) = \sum c_{m_1 \ldots m_n} x_1^{m_1} \ldots\ldots x_n^{m_n}$ theo lối từ điển

là cách sắp xếp các hạng tử của đa thức này theo thứ tự giảm dần hoặc tăng dần của số mũ $(m_1, m_2, \ldots, m_n)$ (theo quan hệ thứ tự ở trên và nếu trong hạng tử thiếu biến x_i thì ta xem $m_i = 0$). Hạng tử với số mũ lớn nhất được gọi là **hạng tử cao nhất của đa thức**.

VÍ DỤ : Trong đa thức $f(x_1, x_2, x_3) = 4x_1^2 x_2^4 + 2x_1 x_3^5 - 3x_1^3 x_2 x_3 + x_2^5 x_3$
ta có $(3,1,1) > (2,4,0) > (1,0,5) > (0,5,1)$ nên có dạng sắp xếp lối từ điển là

$$f(x_1, x_2, x_3) = -3x_1^3 x_2 x_3 + 4x_1^2 x_2^4 + 2x_1 x_3^5 + x_2^5 x_3 .$$

KÍ HIỆU: Nếu $x = (x_1, x_2, \ldots, x_n)$, $m = (m_1, m_2, \ldots, m_n)$ thì ta viết

$$x^m = x_1^{m_1} x_2^{m_2} \ldots x_n^{m_n}$$

2.3 Định lí

Nếu A là vành nguyên thì $A[x_1, x_2, \ldots, x_n]$ cũng là vành nguyên

Chứng minh: Giả sử $f = \sum_{k=0}^{n} a_k x^k$ và $g = \sum_{k=0}^{m} b_k x^k$ là hai đa thức khác 0 và được sắp xếp theo lối từ điển, tức là $n > n-1 > \ldots > 0$, $m > m-1 > \ldots > 0$, và các hạng tử cao nhất của chúng có các hệ tử lần lượt là $a_n \neq 0$, $b_m \neq 0$.
Khi đó $f.g = \sum_{i,j} a_i b_j x^{i+j}$, $i = 1, 2, \ldots, n$ và $j = 1, 2, \ldots, m$. Từ đó hệ tử của hạng tử cao nhất trong f.g là $a_n b_m$. Vì A là vành nguyên nên $a_n b_m \neq 0$, và do vậy $f.g \neq 0$. □

CHÚ Ý: Vành đa thức $K[x_1, x_2, \ldots, x_n]$ trên trường K không phải là vành chính với $n \geq 2$. Chẳng hạn ideal $< x_1, x_2, \ldots, x_n >$ không phải là một ideal chính.

2.4 Đa thức đối xứng

• Cho A là một vành giao hóan với đơn vị $1 \neq 0$, $A[x_1, x_2, \ldots, x_n]$ là vành đa thức n biến . Một đa thức $f \in A[x_1, x_2, \ldots, x_n]$ gọi là đối xứng nếu

$$f(x_1, x_2, \ldots, x_n) = f(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)}) \quad \text{với mọi hóan vị } \sigma \in S_n.$$

• VÍ DỤ: Các đa thức sau đây :

$$\sigma_1 = x_1 + x_2 + \ldots + x_n$$

$$\sigma_2 = x_1x_2 + x_1x_3 \ldots + x_{n-1}x_n$$

. . . . . .

$$\sigma_k = \sum_{1 \leq i_1, .., i_k \leq n} x_{i_1} x_{i_2} \ldots x_{i_k}$$

. . . . . .

$$\sigma_n = x_1x_2 \ldots x_n$$

là đối xứng và gọi là các **đa thức đối xứng cơ bản.**

2.5 Định lí

Các đa thức đối xứng cơ bản là độc lập đại số trên A, tức là, nếu $f(\sigma_1, \sigma_2, \ldots, \sigma_n) = 0$ với $f \in A[x_1, x_2, \ldots, x_n]$ thì $f = 0$.

Chứng minh: Ta chứng minh bằng qui nạp theo n. Trường hợp n = 1 là tầm thường. Giả sử định lí đúng với n –1, ta sẽ chỉ ra nó cũng đúng với n. Thật vậy, giả sử $f \in A[x_1, x_2, \ldots, x_n]$ là đa thức khác 0 và có cấp bé nhất sao cho $f(\sigma_1, \sigma_2, \ldots, \sigma_n) = 0$. Ta viết đa thức $f(x_1, x_2, \ldots, x_n)$ như một đa thức một biến x_n :

$$f = f_0(x_1, x_2, \ldots, x_{n-1}) + f_1(x_1, x_2, \ldots, x_{n-1})x_n + \ldots + f_s(x_1, x_2, \ldots, x_{n-1})x_n^s$$

trong đó $f_i(x_1, x_2, \ldots, x_{n-1}) \in A[x_1, x_2, \ldots, x_{n-1}]$. Hạng tử $f_0(x_1, x_2, \ldots, x_{n-1}) \neq 0$

vì nếu không thì $f = x_n g$, từ đó $0 = f(\sigma_1, \sigma_2, \ldots, \sigma_n) = \sigma_n g(\sigma_1, \sigma_2, \ldots, \sigma_n) = 0$, và do đó $g(\sigma_1, \sigma_2, \ldots, \sigma_n) = 0$, nhưng điều này mâu thuẩn với f là có cấp nhỏ nhất thỏa $f(\sigma_1, \sigma_2, \ldots, \sigma_n) = 0$. Bây giờ ta có

$$0 = f_0(\sigma_1, \sigma_2, \ldots, \sigma_{n-1}) + f_1(\sigma_1, \sigma_2, \ldots, \sigma_{n-1})\sigma_n + \ldots + f_s(\sigma_1, \sigma_2, \ldots, \sigma_{n-1})\sigma_n^s$$

Vế phải tất nhiên là một đa thức n biến $x_1, x_2, \ldots, x_n$ và nếu thay $x_n = 0$ vào thì

do $\sigma_n(x_1, x_2, \ldots, x_{n-1}, x_n) = x_1 x_2 \ldots x_{n-1} 0 = 0$ nên ta có $f_0(\omega_1, \omega_2, \ldots, \omega_{n-1}) = 0$ trong đó $\omega_i = \sigma_i(x_1, x_2, \ldots, x_{n-1}, 0)$ là đa thức đối xứng cơ bản n – 1 biến. Kết hợp với $f_0(x_1, x_2, \ldots, x_{n-1}) \neq 0$ sẽ dẫn đến mâu thuẩn với giả thiết qui nạp. □

2.6 Định lí

Đối với mỗi đa thức đối xứng $f \in A[x_1, x_2, \ldots, x_n]$ tồn tại duy nhất một đa thức $g \in A[x_1, x_2, \ldots, x_n]$ sao cho $f(x_1, x_2, \ldots, x_n) = g(\sigma_1, \sigma_2, \ldots, \sigma_n)$.

Chứng minh:

- *Sự tồn tại.*

. Ta sắp xếp $f(x_1, x_2, \ldots, x_n)$ theo lối từ điển và giả sử $ax_1^{a_1} x_2^{a_2} \ldots x_n^{a_n}$ là hạng tử cao nhất của nó. Khi đó ta phải có $a_1 \geq a_2 \geq \ldots \geq a_n$. Thật vậy, giả sử tồn tại i sao cho $a_i > a_{i-1}$. Vì f đối xứng nên f phải chứa hạng tử $ax_1^{a_1} \ldots x_{i-1}^{a_i} x_i^{a_{i-1}} \ldots x_n^{a_n}$

có được từ $ax_1^{a_1} x_2^{a_2} \ldots x_n^{a_n}$ bằng cách thay x_i bởi x_{i-1} và x_{i-1} bởi x_i . Do $a_i > a_{i-1}$ nên $(a_1, \ldots, a_{i-2}, a_i, a_{i-1}, \ldots, a_n) > (a_1, \ldots, a_{i-2}, a_{i-1}, a_i, \ldots, a_n)$, vậy $ax_1^{a_1} x_2^{a_2} \ldots x_n^{a_n}$ không là hạng tử cao nhất, và điều này dẫn đến mâu thuẩn.

. Xét đa thức $a\,\sigma_1^{a_1-a_2} \sigma_2^{a_2-a_3} \ldots \sigma_n^{a_n}$ và dễ kiểm tra rằng đó cũng là đa thức đối xứng và có hạng tử cao nhất là $ax_1^{a_1} x_2^{a_2} \ldots x_n^{a_n}$.

. Đặt $f_1 = f - a\,\sigma_1^{a_1-a_2} \sigma_2^{a_2-a_3} \ldots \sigma_n^{a_n}$ (rõ ràng nó là đa thức đối xứng)

- Nếu $f_1 = 0$ (đã chứng minh xong)
- Nếu $f_1 \neq 0$, thì ta lại sắp xếp nó theo lối từ điển và giả sử hạng tử cao nhất của nó là $bx_1^{b_1} x_2^{b_2} \ldots x_n^{b_n}$, để ý rằng lúc này $(a_1, a_2, \ldots, a_n) > (b_1, b_2, \ldots, b_n)$, và do đó $a_1 \geq b_1$.

. Đặt $f_2 = f_1 - a\,\sigma_1^{b_1-b_2} \sigma_2^{b_2-b_3} \ldots \sigma_n^{b_n}$

- Nếu $f_2 = 0$ (đã chứng minh xong)
- Nếu $f_2 \neq 0$, thì ta lại sắp xếp nó theo lối từ điển và giả sử hạng tử cao nhất của nó là $cx_1^{c_1} x_2^{c_2} \ldots x_n^{c_n}$, để ý rằng lúc này $(b_1, b_2, \ldots, b_n) > (c_1, c_2, \ldots, c_n)$, và do đó $b_1 \geq c_1$.

. . . . . .

Quá trình trên sẽ chấm dứt sau một số hữu hạn bước vì tương ứng với nó ta có dãy các số tự nhiên giảm dần $a_1 \geq b_1 \geq c_1 \geq \ldots \geq 0$.

- *Sự duy nhất.* Giả sử có g và $g_1 \in A[x_1, x_2, \ldots, x_n]$ sao cho

$$f(x_1, x_2, \ldots, x_n) = g(\sigma_1, \sigma_2, \ldots, \sigma_n) = g_1(\sigma_1, \sigma_2, \ldots, \sigma_n).$$

Khi đó $(g - g_1)(\sigma_1, \sigma_2, \ldots, \sigma_n) = 0$, từ đó $g = g_1$ do định lí 2.5. □

CHÚ Ý: Phép chứng minh sự tồn tại trong định lí cung cấp một phương pháp để tìm g sao cho $f(x_1, x_2, \ldots, x_n) = g(\sigma_1, \sigma_2, \ldots, \sigma_n)$, tức là phương pháp biểu thị một đa thức đối xứng qua các đa thức đối xứng cơ bản.

VÍ DỤ: Biểu thị đa thức đối xứng sau qua các đa thức đối xứng cơ bản

$$f(x_1, x_2, x_3) = x_1^2 x_2 + x_1 x_2^2 + x_1^2 x_3 + x_1 x_3^2 + x_2^2 x_3 + x_2 x_3^2$$

Giải:

Hạng tử cao nhất của f là $x_1^2 x_2$.

Lập hàm $f_1 = f - \sigma_1^{2-1} \sigma_2^{1-0} \sigma_3^0 = f - \sigma_1 \sigma_2$

$$= x_1^2 x_2 + x_1 x_2^2 + x_1^2 x_3 + x_1 x_3^2 + x_2^2 x_3 + x_2 x_3^2$$
$$- (x_1 + x_2 + x_3)(x_1 x_2 + x_1 x_3 + x_2 x_3) = -3 x_1 x_2 x_3$$

Lập hàm $f_2 = f_1 + 3\sigma_1^{1-1} \sigma_2^{1-1} \sigma_3^1 = f_1 + 3\sigma_3 = 0$

Từ đó $f = f_1 + \sigma_1 \sigma_2 = -3\sigma_3 + \sigma_1 \sigma_2$.

3. Các đa thức trên trường số

3.1 Định lí (d' Alermbert)

Trường số phức $\forall$ là đóng đại số, tức là mọi đa thức $f \in \forall[x]$ có bậc ≥ 1 đều có nghiệm trong $\forall$.

Chứng minh: (xem phần phụ lục)

3.2 Định lí

a) Các đa thức bất khả qui trên $\forall[x]$ là các đa thức bậc 1 : $p(x) = ax + b$.

b) Các đa thức bất khả qui trong 3 [x] bao gồm :

- Các đa thức bậc 1 : $p(x) = ax + b$
- Các đa thức bậc 2 : $p(x) = ax^2 + bx + c$ với $\Delta = b^2 - 4ac < 0$.

Chứng minh: a) suy ra trực tiếp từ định lí 3.1. Ta chứng minh b). Giả sử p(x) thuộc 3[x] là bất khả qui và deg(p) $\geq$ 2. Vì p(x) cũng thuộc $\forall$[x] nên theo định lí 3.1 p(x) có ít nhất một nghiệm z $\in \forall$ và do p bất khả qui trong 3 [x] nên z $\notin$ 3 . Vì $\bar{z}$ cũng là nghiệm của p(x) nên T = (x – z)(x – $\bar{z}$) là một ước của p(x) trong $\forall$[x], nhưng T = x^2 – 2Re(z)x + | z | $\in$ 3 [x] nên T cũng là ước của p(x) trong 3[x]. Do p bất khả qui nên T phải liên kết với p, tức là p = a.T, với a $\in 3^*$. Vậy p(x) là một tam thức bậc 2 không có nghiệm thực. Ngược lại rõ ràng các đa thức bậc 1 là bất khả qui, các đa thức bậc 2 không có nghiệm thực cũng vậy, vì nếu không thì nó phải có một ước là đa thức bậc 1 và điều này mâu thuẩn với giả thiết vô nghiệm của đa thức đó. □

3.3 Định lí (tiêu chuẩn Eisenstein)

Nếu f(x) = $a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0 \in 9[x]$ và p là một số nguyên tố thỏa mãn

$a_n \neq 0(\text{ mod } p)$, $a_i \equiv 0(\text{mod } p)$ với mọi i < n, và $a_0 \neq 0 (\text{mod } p^2)$

thì f(x) là đa thức bất khả qui trong Θ[x].

Chứng minh: Giả sử f =g.h, với g = $\sum_{k=0}^{r} b_k x^k$, h $\sum_{k=0}^{s} c_k x^k$; r, s > 0 và r + s = n. Vì $a_0 = b_0 c_0$ và do p nguyên tố thỏa p | a_0 nên suy ra $b_0 \equiv 0(\text{mod } p)$ hoặc $c_0 \equiv 0(\text{mod } p)$. Chú ý rằng nếu $b_0 \equiv 0(\text{mod } p)$ thì $c_0 \neq 0(\text{mod } p)$ vì nếu không thì $a_0 = b_0 c_o \equiv 0(\text{mod } p^2)$. Giả sử $b_0 \equiv 0(\text{mod } p)$. Ta cũng để ý rằng không phải mọi hệ số của g(x) đều là bội của p vì nếu không thì $a_n = b_r c_s \equiv 0(\text{mod } p)$, và điều này trái với giả thiết. Gọi b_i là hệ số đầu tiên của g không chia hết cho p ($0 < i \leq r < n$). Khi đó từ $a_i = b_i c_0 + b_{i-1}c_1 + \ldots + b_0 c_i$ suy ra $b_i c_0 \equiv 0(\text{mod } p)$ nhưng do p nguyên tố nên p $|b_i$ hoặc p | c_0, và điều này dẫn đến mâu thuẩn. □

VÍ DỤ: Nếu p là nguyên tố thì $f(x) = x^m - p$ là đa thức bất khả qui.

BÀI TẬP

1. Trên vành $9_p[x]$ xét đa thức $f(x) = x^p$. Hãy xác định hàm đa thức $\hat{f}$ tương ứng với f.

2. Cho p là số nguyên tố và đa thức $f(x) = x^p - 1 \in 9_p[x]$. Chứng minh rằng $f(x) = (x-1)^p$.

3. Trong vành đa thức $9_5[x]$ hãy thực hiện các phép tóan :

a) $(\bar{2}x^2 + \bar{4}x^2 + \bar{1})(\bar{3}x^2 + \bar{1}x + \bar{2})$
b) $(-\bar{2}x^2 + \bar{4}x + \bar{3})^2$
c) Phép chia $(-\bar{1}x^3 + \bar{2}x^2 + \bar{2}x + \bar{1})$ cho $(-\bar{2}x^2 + \bar{2}x - \bar{1})$

4. Trong vành $9_6[x]$ hãy thực hiện phép nhân

$$(\bar{2}x^3 + \bar{4}x^2 + \bar{1}x)(\bar{3}x^2 + \bar{3}x + \bar{2})$$

5. Trong vành $9_7[x]$ hãy xác định p để dư của phép chia

$(\bar{1}x^3 + \bar{p}x + \bar{5})$ cho $(\bar{1}x^2 + \bar{5}x + \bar{6})$ là bằng 0.

6. Trong vành $\Theta[x]$ chứng minh rằng đa thức $(x+1)^{2n} - x^{2n} - 2x - 1$ chia hết cho các đa thức $2x + 1$, $x + 1$ và x.

7. Chứng tỏ đa thức $\bar{1}x^2 + \overline{14} \in 9_{15}[x]$ có 4 nghiệm trong 9_{15}.

8. Cho các đa thức

$$f(x) = -x^3 - 7x^2 + 2x - 4$$
$$g(x) = -2x^2 + 2x - 1.$$

a) Tìm ƯCLN của f(x) và g(x) trong $\Theta[x]$
b) Tìm ƯCLN của f(x) và g(x) trong $9_{11}[x]$

9. Xét tập $\Theta(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \Theta\}$. Chứng minh rằng

a) $\Theta(\sqrt{2})$ là một trường với phép cộng và nhân thông thường các số.
b) $\Theta(\sqrt{2}) \cong \Theta[x] / _{<x^2-2>}$

10. Xét tập $3(\sqrt{-3}) = \{a + b\sqrt{-3} : a, b \in 3\}$. Chứng minh rằng :

a) $3(\sqrt{-3})$ là một trường với phép cộng và nhân thông thường các so
b) $3(\sqrt{-3}) \cong 3[x]/_{<x^2+3>}$.

11. Hãy biểu diễn các đa thức sau qua các đa thức đối xứng cơ bản

1) $x^3 + y^3 + z^3 - 3xyz$
2) $x^2 y + x y^2 + x^2 z + x z^2 + y^2 z + y z^2$.
3) $x^4 + y^4 + z^4 - 2x^2 y^2 - 2 x^2 z^2 - 2 y^2 z^2$.
4) $x^5 y^2 + x^2 y^5 + x^5 z^2 + x^2 z^5 + y^5 z^2 + y^2 z^5$.

12. Xác định tính bất khả qui của các đa thức sau trên trường số hữu tỉ

1) $x^4 - 8x^3 + 12x^2 - 6x - 2$
2) $x^5 - 12x^3 + 36x - 12$
3) $x^4 - x^3 + 2x + 1$

13. Chứng minh rằng đa thức thuộc $3[x]$ có bậc ≥ 3 đều không bất khả qui.

14. Cho $f(x) = x^n + \ldots + a_0 \in 9[x]$ với $n \geq 1$. Chỉ ra rằng nếu f có nghiệm hữu tỉ thì nghiệm đó là nghiệm nguyên và là ước của a_0.

15. Tìm tất cả các nghiệm hữu tỉ của các đa thức sau:
a) $x^7 - 1$
b) $2x^4 - 4x + 3$
c) $x^5 + x^4 - 6x^3 - 14x^2 - 11x - 3$

16. Cho p là số nguyên tố. Đặt $f(x) = x^p + x^{p-1} + \ldots + 1$. Chứng tỏ rằng f(x) là bất khả qui trêa $\Theta[x]$

PHỤ LỤC

1. Trường số thực

1.1 Lát cắt hữu tỉ

• Giả sử K là một trường trên đó đã xác định quan hệ thứ tự tòan phần " bé hơn " $<$. Ta gọi một **lát cắt trên trường K** là một cặp (A_1, A_2) gồm hai tập con của K thỏa mãn các tính chất :

1) $A_1 \neq \emptyset$, $A_2 \neq \emptyset$.
2) $A_1 \cap A_2 = \emptyset$, $A_1 \cup A_2 = K$.
2) $x < y$ với mọi $x \in A_1$, với mọi $y \in A_2$.

• Ta thấy mỗi lát cắt (A_1, A_2) chỉ có thể thuộc một trong bốn loại sau đây:

1) A_1 có phần tử lớn nhất, A_2 có phần tử bé nhất.
2) A_1 có phần tử lớn nhất, A_2 không có phần tử bé nhất.
3) A_1 không có phần tử lớn nhất, A_2 có phần tử bé nhất.
4) A_1 không có phần tử lớn nhất, A_2 không có phần tử bé nhất.

Lát cắt loại 1 gọi là **lát cắt có bước nhảy**, loại 2 và 3 gọi là **lát cắt có biên**, loại 4 gọi là **lát cắt không biên**.

• Một trường sắp thứ tự tòan phần K gọi là **liên tục** nếu mọi lát cắt trên K đều có biên. Trường số hữu tỉ Θ là một trường không liên tục.

• Gọi 3 là tập hợp tất cả các lát cắt trên trường số hữu tỉ Θ. Chú ý rằng lát cắt trên trường hữu tỉ không thể có bước nhảy.

1.2 Các quan hệ trên 3 .

Cho hai lát cắt $\alpha=(A_1, A_2)$, $\beta=(B_1, B_2) \in 3$

• Hai lát cắt α và β gọi là **bằng nhau**, và viết $\alpha = \beta$, nếu và chỉ nếu

$$A_1 - \{\text{phần tử lớn nhất}\} = B_1 - \{\text{phần tử lớn nhất}\}$$
$$\text{hoặc } A_2 - \{\text{phần tử bé nhất}\} = B_2 - \{\text{phần tử bé nhất}\}$$

Ta qui ước viết lát cắt có biên $\alpha=(A_1, A_2)$ với A_2 không có phần tử bé nhất.

• Ta nói rằng α bé hơn β, và viết $\alpha < \beta$, nếu $A_1 \subset B_1$ và $A_1 \neq B_1$.

Với quan hệ $<$, 3 là một tập được sắp thứ tự toàn phần.

1.3 Phép cộng

$(A_1, A_2) + (B_1, B_2) = (C_1, C_2)$

trong đó, $C_2 = \{(a_2 + b_2)\ ,\ a_2 \in A_2, b_2 \in B_2\}$ và $C_1 = \Theta - C_2$.

Đối với phép cộng phần tử đơn vị là $0 = (O_1, O_2)$, trong đó O_1 là tập các số hữu tỉ không dương và O_2 là tập các số hữu tỉ dương, phần tử nghịch đảo của $\alpha = (A_1, A_2)$ là $-\alpha = (A'_1, A'_2)$, trong đó $A'_2 = \{-r : r \in A_1\}$ và $A'_1 = \Theta - A'_2$.

1.4 Phép nhân

a) Nếu $\alpha = (A_1, A_2)$, $\beta = (B_1, B_2) > 0$, thì phép nhân được xác định bởi

$$\alpha.\beta = (A_1, A_2).(B_1, B_2) = (C_1, C_2),$$

ở đây $C_2 := \{a_2.b_2 : a_2 \in A_2, b_2 \in B_2\}$ và $C_1 = \Theta - C_2$.

b) Nếu $\alpha > 0$, $\beta < 0$ hoặc $\alpha < 0$, $\beta > 0$ thì phép nhân được xác định bởi

$$\alpha.\beta = \alpha(-\beta) = (-\alpha)\beta.$$

c) Nếu $\alpha > 0$, $\beta < 0$ thì phép nhân được xác định bởi

$$\alpha.\beta = (-\alpha).(-\beta)$$

d) Nếu $\alpha = 0$ hoặc $\beta = 0$ thì phép nhân được xác định bởi

$$\alpha.\beta = 0.\beta = \alpha.0 = 0$$

Đối với phép nhân phần tử đơn vị có dạng $E = (E_1, E_2)$, trong đó E_1 là tập các số hữu tỉ không lớn hơn 1 và E_2 là tập các số hữu tỉ lớn hơn 1, phần tử nghịch đảo của $\alpha = (A_1, A_2) > 0$ là $\alpha^{-1} = (A'_1, A'_2)$, trong đó tập $A'_2 = \{r^{-1} : r \in A_1, r > 0\}$ và $A'_1 = \Theta - A'_2$, còn phần tử nghịch đảo của $\alpha < 0$ là $\alpha^{-1} = (-\alpha)^{-1}$.

2. Trường số phức

2.1 Xây dựng số phức

• Ta xét tập hợp $\forall = 3 \times 3$ là tập tất cả các cặp số thực (a, b) mà trên đó quan hệ bằng nhau, phép tóan cộng, phép tóan nhân được xác định như sau :

$(a, b) = (c, d) \Leftrightarrow a = b$ và $c = d$.

$(a, b) + (c, d) = (a + c, b + d)$

$(a, b) . (c, d) = (a\,c - b\,d, a\,d + b\,c)$.

• Đối với phép cộng phần tử đơn vị là **0** = (0, 0), phần tử nghịch đảo của z = (a, b) là – z = (– a, – b). Đối với phép nhân phần tử đơn vị là **1** =(1, 0), phần tử nghịch đảo của z =(a, b)≠ **0** là $z^{-1} = (\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2})$.

Với phép cộng và phép nhân đã được định nghĩa thì (∀,+,•) là một trường, gọi là **trường số phức,** mỗi phần tử gọi là một **số phức**.

• Nếu đặt $\forall_0 = \{(a, 0): a \in 3\} \subset \forall$ thì (∀, +, •) là một trường và từ đẳng cấu $\varphi : 3 \to \forall_0, a \mapsto (a, 0)$, ta có thể đồng nhất 3 với $\forall_0$, tức là mỗi số thực x ∈ 3 đồng nhất với số phức (x, 0) ∈ ∀ , đặc biệt 1 ≡ (1, 0), và 0 ≡ (0, 0).

• Với mỗi số phức z = (a, b) ∈ ∀, ta có thể viết :

$$(a, b) = (a, 0) + (b, 0).(0, 1)$$

và nếu đặt i = (0, 1) thì số phức z có dạng z = a + bi, gọi là dạng đại số của số phức. Số a được gọi là **phần thực** của số phức z, kí hiệu a = Rez, và số b được gọi là **phần ảo** của số phức z, kí hiệu b = Im z. Ta gọi số phức $\bar{z}$ = a – bi là số phức liên hợp của số phức z = a + bi. Việc tính toán các số phức viết dưới dạng đại số như tính toán trên số thực với chú ý rằng

$$i^2 = i.i = (0, 1).(0, 1) = (-1, 0) \equiv -1$$

• Nếu trên mặt phẳng tọa độ Oxy ta đặt tương ứng mỗi số phức z = a + bi với điểm M(a,b) ∈ Oxy hoặc với vectơ $\overrightarrow{OM}$ = (a, b) ∈ mpOxy thì ta được một song ánh từ ∀ lên mpOxy. Điểm M(a,b) hoặc vectơ $\overrightarrow{OM}$ = (a,b) được gọi là **biểu diễn hình học của số phức** z. Mặt phẳng tọa độ Oxy còn được gọi là **mặt phẳng phức**, trục Ox gọi là trục thực, Oy là trục ảo.

• Bây giờ giả sử z = a + bi là một số phức bất kì được biểu diễn bởi vectơ $\overrightarrow{OM}$ trên mp Oxy. Ta gọi $r = |\overrightarrow{OM}| = \sqrt{a^2+b^2}$ là **modul của số phức** z, và kí hiệu | z |. Góc định hướng (Ox, $\overrightarrow{OM}$) gọi là **argument** của của số phức z, kí hiệu arg z. Ta thấy rằng số 0 có modul là 0 và argument tùy ý, còn mỗi số phức khác 0 có modul là một số thực dương và argument được xác định sai khác nhau một bội nguyên của 2π.

• Nếu số phức z = (a,b) ≠ 0 có | z | = r và arg z = φ (hoặc tổng quát arg z = φ +k2π) thì ta có một biểu diễn khác của số phức như sau (gọi là biểu diễn lượng giác)

$$z = (a,b) = a + bi = r(\cos\varphi + i\sin\varphi)$$

- Với $z = r(\cos\varphi + i\sin\varphi)$, ta có các công thức

$$z^n = [r(\cos\varphi + i\sin\varphi)]^n = r^n(\cos n\varphi + i\sin n\varphi)$$

$$\sqrt[n]{z} = \sqrt[n]{r}\left(\cos\frac{\varphi + 2k\pi}{n} + i\sin\frac{\varphi + 2k\pi}{n}\right), \quad k = 0, 1, 2, \ldots, n-1.$$

2.2 Định lí (d' Alermbert)

Trường số phức $\forall$ là đóng đại số, tức là mọi đa thức $f \in \forall[z]$ có bậc ≥ 1 đều có nghiệm trong $\forall$.

Chứng minh: Có nhiều phép chứng minh định lí d'Alermbert và thường phải sử dụng đến kết quả của giải tích. Sau đây là một. Ta sẽ chứng minh bằng phương pháp phản chứng: Giả sử tồn tại một đa thức $f(z) = \sum_{i=0}^{n} a_i z^i \in \forall[x]$ khác hằng và không có nghiệm nào trong $\forall$. Xét hàm

$$|f| : \forall \to \forall, x \mapsto |f(z)|$$

Vì $|f| \to \infty$ khi $|z| \to \infty$ nên tồn tại $R > 0$ sao cho $|f(z)| > |f(0)|$ với mọi $z \in \{|z| > R\}$. Vì $|f|$ liên tục trên compact $\{|z| \leq R\}$ nên tồn tại $z_0 \in \forall$ sao cho $|f(z_0)| = \min_{|z| \leq R} |f(z)|$. Nhưng vì $|f(z)| > |f(0)| \geq |f(z_0)|$ với mọi $z \in \{|z| > R\}$ nên ta có $|f(z_0)| = \min_{z \in C} |f(z)|$.

Ta có công thức Taylor đối với f

$$f(z_0 + h) = f(z_0) + h f'(z_0) + \ldots + \frac{h^n}{n!} f^{(n)}(z_0)$$

Ta chứng minh rằng, có thể chọn h sao cho $|f(z_0 + h)| < |f(z_0)|$ và từ đó suy ra mâu thuẩn. Trước hết để ý rằng, có ít nhất một đạo hàm cấp cao của f tại z_0 là khác 0, cụ thể là $f^{(n)}(z_0) = n!a_n \neq 0$. Gọi $k \geq 1$ là số nguyên bé nhất sao cho $f^{(k)}(z_0) \neq 0$. Như vậy ta có

$$\frac{f(z_o + h)}{f(z_0)} = 1 + h^k \frac{f^{(k)}(z_o)}{k!f(z_0)} + \ldots + h^n \frac{f^{(n)}(z_o)}{n!f(z_0)}$$

$$= 1 + h^k \frac{f^{(k)}(z_o)}{k!f(z_0)} + h^{k+1} g(h), \text{ với } g(h) \in \forall[h] \text{ nào đó.}$$

Gọi w là số phức sao cho $w^k = -\dfrac{f^{(k)}(z_o)}{k!f(z_0)}$, khi đó ta có

$$\frac{f(z_o + \frac{t}{w})}{f(z_0)} = 1 - t^k + t^{k+1}w^{-k-1}\, g(tw^{-1}).$$

Vì hàm một biến $f_1(t) = |\, w^{-k-1}\, g(tw^{-1})|$ liên tục trên $[0, 1]$) nên tồn tại $C > 1$ sao cho với mọi $t \in [0, 1]$ ta có $|\, w^{-k-1}\, g(tw^{-1})| < C$, và từ đó

$$\left| \frac{f(z_o + \frac{t}{w})}{f(z_0)} \right| \le 1 - t^k + C\, t^{k+1}.$$

Bây giờ chỉ cần chọn t sao cho $0 < t < \dfrac{1}{C} < 1$ thì ta có

$$0 < 1 - t^k + C\, t^{k+1} < 1.$$

hay $|\, f(z_0 + \frac{t}{w})\,| < |\, f(z_0)\,|$ □